VŠB TECHNICKÁ UNIVERZITA OSTRAVA
FAKULTA ELEKTROTECHNIKY A INFORMATIKY

Automatizace a bezpečnost infrastruktury

Automation and Security of Infrastructure

Matěj Nedojedlý

Diplomová práce

Vedoucí práce: Ing. Lukáš Vojáček, Ph.D.

Ostrava, 2021

Abstrakt

Diplomová práce se zaměřuje na bezpečnost a automatizaci síťové infrastruktury. Práce poukazuje na důležitost těchto vlastností v infrastruktuře. Obsahuje zmapování nástrojů pro bezpečnostní audity a automatizovanou správu systémů. Dalé zahrnuje instalaci a konfiguraci vybraných nástrojů pro vytváření bezpečnostních auditů. Druhá část práce popisuje instalaci a konfiguraci softwaru System Center Configuration Manager. Zahrnuje konfiguraci automatických aktualizací pro Windows a také nasazení automatické instalace Windows Serverů s předpřipraveným nastavením.

Klíčová slova

infrastruktura; automatizace; bezpečnost; Suricata; OpenVAS; System Center Configuration Manager; automatizovaná správa systémů

Abstract

The diploma thesis is focused on security and automation of network infrastructure. The diploma thesis points out the importence of these properties in infrastructure. It includes mapping of security audit tools and tools for automated system management. It also includes the installation and configuration of selected tools for creating security audits. The second part of diploma thesis describes the installation and configuration of the System Center Configuration Manager. It includes configuration of automatic updates for Windows and also deployment of automatic installation of Windows Server with pre-sets.

Keywords

infrastructure; automation; security; Suricata; OpenVAS; System Center Configuration Manager; automated system management

Poděkování

Rád bych na tomto místě poděkoval všem, kteří mi s prací pomohli, protože bez nich by tato práce nevznikla. Především mému vedoucímu práce panu Ing. Lukáši Vojáčkovi, Ph.D. za odborné vedení mé diplomové práce a také za znalosti, které mi během práce předal.

Obsah

Seznam použitých zkratek a symbolů

IDS	–	Intrusion Detection System
IRC	–	Internet Relay Chat
HIDS	–	Host-Based Intrusion Detection System
NIDS	–	Network Intrusion Detection System
IPS	–	Intrusion Prevention Systems
TLS	–	Transport layer security
TCP	–	Transmission Control Protocol
UDP	–	User Datagram Protocol
VPN	–	Virtual private network
IP	–	Internet Protocol
ICPM	–	Internet Control Message Protocol
SSH	–	Secure Shell
IT	–	Information technology
SCCM	–	System Center Configuration Manager
NVMe	–	Non-Volatile Memory express
NVDIMM	–	Non-Volatile Dual In-line Memory Module
AD	–	Active Directory
WSUS	–	Windows Server Update Services

Seznam obrázků

Seznam tabulek

Kapitola 1

Úvod

Automatizace a bezpečnost v síťové infrastruktuře jsou velmi důležité pojmy. S rostoucí infrastrukturou rostou požadavky na zabezpečení a automatizaci správy systémů. Zabezpečení infrastruktury se skládá například z brány firewall, Virtual Privete Network, řízení přístupu a další. Diplomová práce je zaměřena na prevenci těchto napadení na využívání IDS nástrojů nebo nástrojů, které slouží skenování zranitelností v síti. Automatizace je důležitá ve větších infrastrukturách, aby byla udržena jistá integrita mezi servery. Servery požadují pravidelnou údržbu, která zahrnuje například pravidelné aktualizace nebo zálohu. Diplomová práce je zaměřena na automatickou správu serverů, které používají operační systém Windows od společnosti Microsoft.

První kapitola vás uvede do této problematiky. Jsou zde popsány základy síťové bezpečnosti a základy o zabezpečovacích softwarech. Druhá část této kapitoly pojednává o automatizaci a nastínění možných nástrojů, které usnadňují chod síťové infrastruktury.

V druhé kapitole jsou představeny parametry síťové infrastruktury, na které je práce implementována. Jedná se o infrastrukturu, která je vyvíjená v rámci H2020 projektu LEXIS. V první části této kapitoly jsou představeny hardwarové parametry a virtualizační nástroje. V druhé části jsou uvedeny softwarové nástroje, které se vztahují k této diplomové práci.

Následující kapitola je zaměřena na analýzu nástrojů, které provádí bezpečnostní audity. Na začátku kapitoly jsou uvedeny různé IDS nástroje, kde je popsána jejich základní funkčnost. V další části kapitoly jsou popsány nástroje, které se zabývají hledáním zranitelností v systémech, pomocí skenování daného serveru. V této části jsou uvedeny rozdíly mezi různými nástroji.

Kapitola číslo čtyři je zaměřena na teoretickou část automatizace infrastruktury. Jsou zde popsány různé nástroje, které administrátorům pomohou se správou většího počtu serverů. Nejrozsáhlejší rozbor má nástroj System Center Configuration Manager od společnosti Microsoft, který je použit v této práci.

Diplomová práce pokračuje instalací a konfigurací nástroje OpenVAS, který slouží jako skener zranitelností v systémech. V kapitole je detailně popsána instalace a konfigurace nastavení pro automatické skenování těchto zranitelností na vybraných serverech. Po úspěšné konfiguraci je popsán

právě výpis tohoto skenování a je představen výpis této aktivity. V rozebraném výpisu jsou uvedeny informace, které z něj lze vyčíst. V další části je popsána instalace a konfigurace IDS nástroje Suricata. Bude sloužit ke sledování síťového provozu v infrastruktuře na všech jeho rozhraních. Detailně je popsána instalace a globální konfigurace tohoto nástroje. Je představena konfigurace této služby na specifické rozhraní a představení využívaných pravidel pro sledování síťového provozu. V závěru této kapitoly je představen zachycený výpis z proběhlého sledování provozu.

Poslední kapitola je zaměřena na software System Center Configuration Manager. První část této kapitoly je zaměřena na instalaci tohoto nástroje. Je zde detailně uveden celý postup instalace a také následná počáteční konfigurace. V konfiguraci jsou popsány všechny nutné kroky, aby mohl nástroj plně využívat téměř všechny nabízené funkce. První funkce, která je v diplomové práci popsána je nastavení automatických aktualizací pro servery s operačními systémy Windows. Tato část je pro infrastrukturu velmi důležitá, jelikož udržovat servery aktuální je hlavním krokem v cestě za zabezpečenou infrastrukturou. Další části kapitoly je automatické nasazení operačních systémů. Detailně je popsána konfigurace samotného konfiguračního manažera, tak i konfigurace DHCP serveru pro možnost bootování přes PXE. Funkce automatického nasazení operačních systému ušetří práci s instalací nového serveru v infrastruktuře.

Kapitola 2

Bezpečnost a automatizace

Úvodní kapitola vás uvede do problematiky síťové bezpečnosti. V druhé části této kapitoly budou popsány důvody automatizace v infrastrukturách a nástroje, které se touto problematikou zabývají.

2.1 Síťová bezpečnost

Podkapitola je zaměřena na začátky síťové bezpečnosti a obecný pohled na systémy pro odhalování bezpečnostních hrozeb. Bude představena základní architektura těchto systémů a jejich možné typy, které jsou k dispozici.

Již v počátcích vzniku síťové komunikace se uvažovalo o nějakém typu zabezpečení. Do devadesátých let byl internet relativně nepoužívaný veřejností. V té době zabezpečení nebylo na vysoké úrovni, to se však s rostoucími citlivými informacemi začalo měnit.

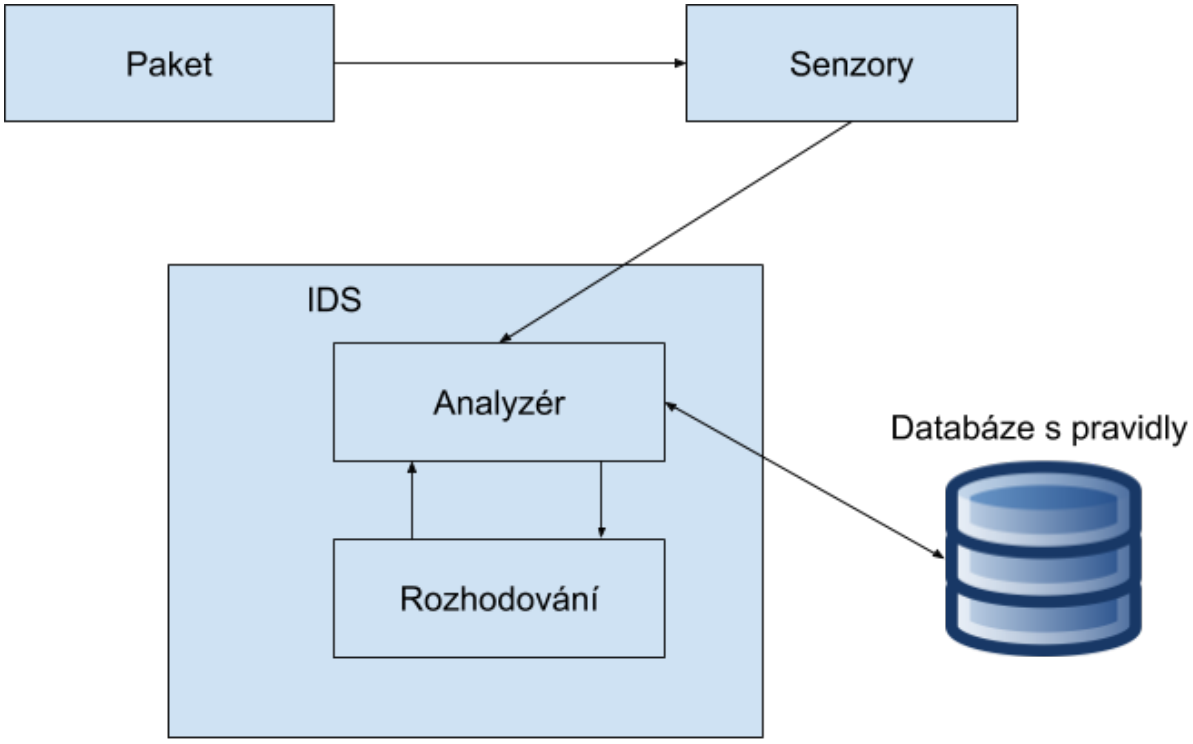
Koncem 80. let se zvedl počet uživatelů, kteří začali využívat internet. Připojili se univerzity, vládní a vojenská zařízení. Díky této události začala růst potřeba po zabezpečení. V roce 1988 byl vypuštěn první automatizovaný červ zvaný *Morris Worm*. Byl vyvinut studentem, který využil nedostatku systémové prevence pro narušení. Díky tomu se mohl připojit k infikovanému počítači a využít chyby v zabezpečení k vlastnímu kopírovaní souboru apod. Po tomto incidentu se vláda rozhodla zakročit a začala pracovat na vývoji týmu zvaný CERT, nebo-li *Computer Emergency Response Team*. Jednalo se o první organizaci, která se zabývala zabezpečením sítě. Zrušením komerčního práva pro ARPANET, dnes již známý jako internet, došlo k rychlému rozšíření mezi běžné uživatele. Sítě se stali velkým lákadlem pro hackery po celém světě. [1, 2]

2.1.1 Využití Intrustion Detection System

Jednou z mnoha možností, jak zajistit lepší síťovou bezpečnost je využití Intrustion Detection System (IDS), neboli systém pro odhalení bezpečnostních hrozeb. O základ vývoje IDS se postaralo americké letectvo. V roce 1980 napsal James P. Anderson zprávu *Computer Security Threat Moni-*

toring and Surveillance, což se stalo základem pro zavedení automatizovaného IDS. Brzy po vydání zprávy byl vyvinut první model IDS. Jednalo se o systém, založený na daných pravidlech, které porovnávají síťový provoz se seznamem známých hrozeb. IDS software se dají rozdělit na dva typy a to HIDS (Host-based Intrustion Detection System) a NIDS (Network Instrustion detection system). Důvodem, proč využívat IDS systémy v infrastrukturách, je včasné upozornění na dějící se podezřelou aktivitu. Systémy IDS lze porovnat se systémy IPS (Intrustion prevece system). Rozdíl mezi IDS a IPS je ten, že zatím co systémy IDS pouze detekují a zaznamenávají danou hrozbu, tak systémy IPS brání v jejich provedení. Na trhu je spousty nástrojů, které částečně kombinují tyto dva typy nástrojů. [3, 1]

Postupem času se pravidla rozšiřovala a aktualizovala, neboť nových útoků a hrozeb v systémech a sítích přibývá. V dnešní době hledají hackeři skulinky v aktualizacích softwarů, chyb na straně webových stránek apod.. Vývojáři se všechny tyto skuliny snaží objevit a vložit do pravidel pro zdokonalení jejich nástroje.



Obrázek 2.1: Základní architektura IDS

Na obrázku číslo 2.1 lze vidět základní funkčnost IDS systému. Paket, který dorazí do analyzátoru si vyžádá z databáze pravidla nastavené pro dané IDS. Poté dojde k rozhodnutí, zda-li systém na daný paket vytvoří upozornění, nebo bude přijat bez další aktivity. [3, 1]

2.2 Automatizace

Význam automatizace je zavedení samočinných zařízení bez větší nutnosti asistence člověka. Podkapitola se zaměřuje na automatizaci infrastruktury a popisuje možné nástroje, které je možné pro automatizaci využít.

2.2.1 Automatizace infrastruktury

Automatizace infrastruktury využívá technologie, která provádí úkoly se sníženou lidskou pomocí za účelem řízení hardwaru, softwaru, operačních systémů a síťových komponentů. Důvodem využívání této technologie jsou neustále rostoucí IT organizace, kde se infrastruktury zvětšují a přibývá na jejich složitosti. S omezeným časem a personálem, se snaží držet krok s růstem organizace. Následkem jsou opožděné aktualizace a opravy, tím se výrazně snižuje bezpečnost a funkčnost dané infrastruktury. Použití automatizace na běžné úkony jako jsou aktualizace, konfigurace, nasazování a vyřazování z provozu, dokáže zjednodušit a zajistit integritu celé infrastruktury. Další výhodou je snížení počtu chyb způsobených lidským faktorem. Automatizace je klíčem k optimalizaci celé infrastruktury. [4]

2.2.2 Nástroje pro automatizaci infrastruktury

Jak bylo již uvedeno v dnešní době se žádná infrastruktura neobejde bez určitých softwarů zabývající se automatizací. Na trhu je spoustu softwarů, které se zabývají automatizací. Zde je vybráno pár užitečných nástrojů, které se řadí mezi ty nejpoužívanější.

- **Ansible** - Jedná se o software od společnosti Red Hat. Ansible automatizuje řadu IT úkonů, včetně správy automatizace, zajišťovaní cloudů, nasazování aplikací apod. Ansible lze snadno spravovat pomocí webového rozhraní Ansible Tower. Cena se pohybuje od 5000-14000 dolarů ročně. Výhodou však je, že toto webové rozhraní není nutné využívat pro zajištění automatizace. [5]
- **Jenkins** - Nástroj slouží k vytváření automatizovaných *cloudových pipiline* CI/CD (Continuous integration/continuous delivery), založených na postupech DevOps a na využití Kubernetes. DevOps je kombinací praktik a nástrojů určených ke zvýšení možnosti organizace. Díky nástroji Jenkins můžete zjednodušit vytváření a poskytovaní softwarových produktů pomocí automatizace, cílených vývojových prostředích a dalších. Umožňuje vývojářům soustředit se na vyvíjený kód, místo kontroly, jak je transformován na výstupy a možnostmi jeho nasazení. Vytvoří kanál, který se stane primárním nástrojem pro získávání kódu, místo toho, aby byl kanál překážkou pro doručení. [6, 5]
- **System Center Configuration Manager** - Nástroj vyvíjen společností Microsoft. Pomocí tohoto nástroje můžou být servery v infrastruktuře hromadně aktualizovány, nasazovány nové

aplikace, distribuovány modifikované obrazy s operačním systémem, či spravován antivirus apod. Nástroj je výhradně zaměřen na operační systémy Windows. Podrobnější rozbor o tomto nástroji se dočtete v následujících kapitolách. [7, 5]

Kapitola 3

Infrastruktura projektu

Cílem práce je návrh a implementace IDS řešení a automatizace na konkrétní infrastruktuře. Diplomová práce se vztahuje k infrastruktuře jednoho reálného projektu. Infrastruktura slouží jako testovací prostředí pro orchestrační platformu Cloud and HPC vyvíjenou v rámci H2020 projektu LEXIS [8]. Tato kapitola slouží k obeznámení, jaké hardwarové a softwarové komponenty jsou použity. Kapitola je rozdělena do dvou podkapitol, ve kterých jsou popsány jednotlivé úrovně infrastruktury.

3.1 První úroveň - Hardware

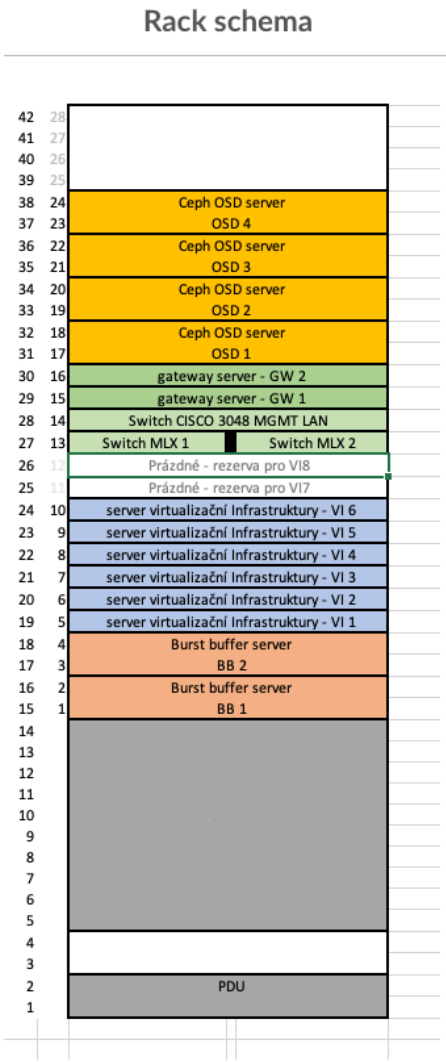
Základem této infrastruktury je šest virtualizačních serverů, které se skládají ze čtyřiceti jádrového procesoru Intel Xeon Gold a velikost operační paměti je 192GB.

Další částí infrastruktury jsou dva *Burst Buffer* servery, nebo-li servery nárazové vyrovnávací paměti. *Burst Buffery* jsou umístěny mezi *front-end* virtualizačními servery a *back-end* uložišti. Servery se také skládají ze čtyřiceti jádrového procesoru Intel Xeon Gold a velikost operační paměti je také 192GB. Pro uložiště na *Burst Bufferu* je zvolen NVMe Intel SSD s pamětí 12,8TB a NVDIMM o velikosti 256GB. Jedná se o energeticky nezávislou paměť, která uchová data i při výpadku elektrické energie nebo pádu systému.

Hlavní úložiště se skládá ze čtyř CEPH OSD serverů. Jejich hrubá kapacita je 180TB úložného prostoru a 60TB slouží jako redundantní paměť. CEPH je open-source software pro úložnou platformu. Poskytuje rozhraní, kde na jednom místě umožňuje spravovat objektové, blokové a file-level uložiště.

Poslední hardwarovou částí je síť, která musí odpovídat výpočetní rychlosti ostatních prvků. V infrastruktuře jsou použity dva *Mellanox* přepínače. Je využita 100 gigabitová linka, která se stará o přenos dat mezi virtualizačními servery a *Burst Buffery*. Dále se tato linka využívá pro komunikaci s gateway servery. K CEPH úložišti vede 25 gigabitová linka, která plně pokryje maximální rychlost čtení a zápisu. Dále se využívají dva InfiniBandy, pro komunikaci mezi *HPC Clustry*, *Burst Buffery*

a *Gateway Servery*. InfiniBand je komunikační standard počítačové sítě využíván u vysoce výkoných počítačů. Vyznačuje se velmi vysokou propustností a velmi nízkou odezvou. Na obrázku číslo 3.1 je schéma racku, ve kterém jsou uvedeny všechny hardwarové komponenty. Pro virtualizaci se využívá software VMware a Openstack.



Obrázek 3.1: Schéma racku infrastruktury

3.1.1 VMware vSphere

VMware je společnost, která nabízí řadu nástrojů. Neslouží výhradně pro virtualizaci, ale také pokrývá technologie, které se zabývají digitální transformací. S více než 500 000 zákazníky zůstává ve světe osvědčeným lídrem. V infrastruktuře se využívá jejich produkt vSphere, který umožňuje řídit virtualizaci a vytvářet nové virtualizované servery. První verze hypervizoru ESXi byla vydána

již v roce 2001 a první verze vCenter byla vydána o dva roky později v roce 2003. Sada VMware vSphere zahrnuje v sobě hypervizor ESXi pro virtualizační vrstvu, tak právě i zmíněný vCenter, který nabízí rozhraní pro správu těchto virtuálních počítačů. Společnost VMware se zaměřuje na čtyři hlavní IT priority v oblasti digitální transformace.

- Modernizace datových center
- Integrace veřejných cloudů
- Zkvalitnění digitálního pracovního prostoru
- Zabezpečení digitální transformace

Právě na výše uvedených prioritách staví při vývoji jejich produktů. VMware vSphere nabízí, přehledné webové grafické rozhraní, které zjednodušuje jakoukoliv práci s vytvářením nových virtuálních serverů, či správou již bežících strojů. [9]

3.1.2 OpenStack

Cloud Computing je o poskytování různých typů infrastrukturních služeb, jako například Software jako služba (SaaS), Platforma jako služba (PaaS), nebo Infrastruktura jako služba (IaaS). OpenStack je open-source nástroj, který umožňuje nasazení a správu cloudové infrastruktury jako službu IaaS. Podporuje nasazení soukromého i veřejného cloudu. OpenStack splňuje dva hlavní požadavky cloudu, kterou je škálovatelnost a jednoduchost implementace. Nabízí vysokou konfigurovatelnost, uživatel si může vybrat, zda bude implementovat několik služeb nabízeným softwarem. Konfigurace každé komponenty je také na uživateli a lze jí snadno provést pomocí API, který nástroj nabízí. Existuje tedy mnoho různých způsobů, jak tento software využívat, což z něj činí flexibilní nástroj, který je schopen spolupracovat s dalšími softwary. OpenStack podporuje různé typy hypervizorů například VMware, Xen, či virtuální stroj založený na jádře KVM a podporuje také několik virtualnizačních technologií. Stručně řečeno, OpenStack umožňuje automatické nasazení a správu cloudové architektury, kterou lze snadno integrovat do jiného softwaru. [10, 11, 12]

3.2 Druhá úroveň - Softwarové nástroje

V této podkapitole bude popsáno, jakým způsobem jsou řešeny základní funkce infrastruktury. Budou popsány různé nástroje, které infrastruktura využívá a jaké nabízí možnosti pro realizaci diplomové práce.

3.2.1 Softwarový firewall - pfSense

Software, který umožňuje správu vnitřní sítě a řeší její zabezpečení. PfSense běží na operačním systému FreeBSD. FreeBSD je odnož BerkleyUNIX vyvinutou univerzitou Berkeley v Kalifornii.

Zkratka pf ve slově pfSense, představuje paketový filtr pro OpenBSD. Byl vymyšlen jako náhrada za IPFilter, který OpenBSD dosud používalo. První verze samotného pfSense 1.0 vyšla v roce 2006 a od té doby vyšla řada aktualizací. Používá se nejnovější verze, která je verzí 2.5. V aktualizacích se objevuje především rušení podpory zastaralých technologií a podpora nově příchozích. PfSense se řadí mezi nejpopulárnější firewall-router s otevřeným zdrojovým kódem a velkou vývojářskou komunitou. Instalace a konfigurace je poměrně snadná a dokáže se zakomponovat do různých typů infrastruktur. Software má vlastní webové rozhraní, které velmi usnadňuje jakoukoliv práci s nabízenými funkcemi. Velkým plusem pfSense je možnost doinstalování speciálních balíčků přímo ve webovém rozhraní a rozšířit tak funkce tohoto nástroje. V této infrastruktuře se využívá pfSense jako firewall, DHCP server, NTP a další. [13]

3.2.2 Adresářová služba - Active Directory

Active Directory je adresářová služba vyvinutá společností Microsoft. Ukládá údaje o identitě organizace do centrálního úložiště a umožňuje nám je uspořádat do hierarchické organizační struktury tak, aby vyhovovaly potřebám podniku. Mimo to, že dokáže uchovávat informace o objektech, jako jsou počítače, uživatelské účty, umožňuje správcům globálně nasazovat systémové politiky, či instalovat aplikace na dané počítače. Výhodou Active Directory je, že dokáže spolupracovat i s jinými operačními systémy než jsou operační systémy od firmy Microsoft. Služba Active Directory se skládá z více služeb: [14]

- **Domain Services** - Základním kamenem každé Windows domény. Ukládá informace o objektech uložené v doméně, ověřuje jejich údaje a definuje přístupová práva.
- **Lightweight Directory Services** - Tato služba umožňuje implementaci LDAP protokolu pro Active Directory Domain Services.
- **Certificate Services** - Zajišťuje vlastní infrastrukturu pro správu veřejných klíčů.
- **Federation Services** - Jedná se o službu, která zajišťuje jednotné přihlášení.

Kapitola 4

Analýza nástrojů pro bezpečnostní audity

V této kapitole je uvedeno několik známých nástrojů, které je možné použít pro bezpečnostní audity. Nástroje jsou mezi sebou porovnány, aby bylo zjištěno, čím se mezi sebou liší a mohl být vybrán ten nejvhodnější nástroj.

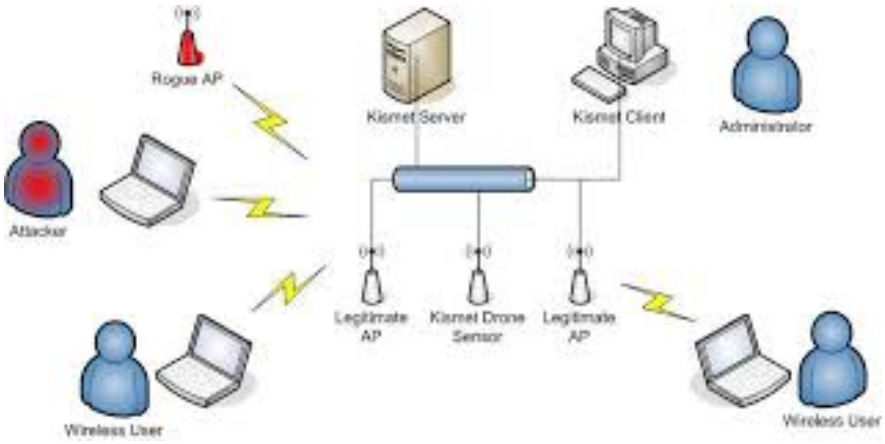
4.1 Rozbor IDS nástrojů

Řada firem nabízí své IDS nástroje, proto je důležité vybrat si nástroj, který bude pro danou firmu ten nejvhodnější. Pro řadu menších firem je důležité, aby neplatili za zabezpečení velké peníze. V tomto rozboru nástrojů byly vybrány jedny z nejznámějších IDS nástrojů.

4.1.1 Kismet

Kismet je open-source software. Jedná se o bezdrátový Intrustion Detection System, který je zaměřen na bezdrátové protokoly jako je Bluetooth, Wi-Fi, s potřebným hardwarem SDR(software defined radio), jako je například RTL-SDR . Kismet běží na operačním systému Linux, OSX a částečně na Windows 10 v rámci WSL frameworku. Na systému Linux funguje s téměř všemi typy Wi-Fi karet, podporuje rozhraní Bluetooth a další hardwarová zařízení. U systému OSX pracuje s vestavěným rozhraním Wi-Fi a u systému Windows 10 bude fungovat s dálkovým snímáním. [15]

Síťové prostředí má určité legitimní body připojení (Access point, AP), které využívají uživatelé bezdrátové sítě. V tomto řešení architektury (obrázek 4.1) jsou umístěny drony Kismet, které se starají o sběr informací ohledně provozu. Drony jsou připojeny ke Kismet serveru a přes síť mu zasílají sesbíraná data. Kismet je náhradou pro malé a střední firmy, které si nemohou dovolit nabídku od komerčních konkurenčních softwarů, jako jsou AirDefense nebo AirMagnet. Tyto dokáží pracovat o něco jednodušeji dokáží, využít již vytvořené legitimní body připojení a není nutno zprovozňovat drony pro sběr informací. Schopností je tedy odkrývat neautorizované přístupové body, dále detekuje konfigurační mezery, skoky kanálů a defaultní síť. Podpora je dostupná na



Obrázek 4.1: Architektura softwaru Kismet [16]

komunitním Discord serveru a na IRC. Je možné si přečíst také dokumentaci, kterou mají uloženou na svých webových stránkách.

Hlavní nevýhodou softwaru Kismet je pomalé vyhledávání, které dokáže zabrat nějaký čas navíc. Kismet velmi dobře běží na zařízeních s operačními systémy Android a iOS, ale podpora pro Windows je limitována. Tento typ IDS nabízí skvělé bezplatné řešení problematiky hlídání provozu u bezdrátových komunikací. Software neodpovídá požadavkům, které byly nastaveny, i když tento nástroj poskytuje mnoho funkcí. [16, 15]

4.1.2 Sagan

Sagan je dalším představitelem open-source řešení v oblasti IDS nástrojů. Byl navržen s ohledem na SOC (Security Operating Center). Nástroj je zaměřen na analýzu protokolů. Software nabízí velký výkon. Nabízí také možnost provádět analýzu záznamů v reálném čase, neboť zpožděná analýza dává výhodu útočníkovi v tom, že během této prodlevy, byly ve vaší síti nezjištěni. Využívá *multi-thereaded* přístup k usnadnění nastavení optimální úrovně výkonu. Sagan využívá minimum procesoru a paměti, taktéž je kompatibilní s běžnými grafickými konzolemi zabývající se zabezpečením. Program je komplexní, proto může nějakou dobu trvat, než se jej obsluha naučí plně využívat. Aplikace je velice podobná nástrojům Suricata a Snort. Dokáže korelovat události protokolu se systémem Suricata a Snort. Dokáže tedy zapisovat do databází od nástroje Snort. K detekci hrozeb může taktéž využít soubor pravidel od společnosti Snort.

Sagan je považován jako analyzátor záznamů, tudíž je jako systém IDS přehlížen, ale díky kombinací přístupů HIDS a NIDS, lze jej využít jako hybridní nástroj. Jako hlavní nevýhody je považována náročnost pro nové správce bezpečnostní sítě a nezaměřenost na právě jeden z přístupů. [17, 18]

4.1.3 Suricata

Software Suricata je velmi sofistikovaný a velmi rychlý IDS systém. Jedná se o další open-source řešení, které patří mezi ty nejvyužívanější. Poskytuje kombinaci dvou funkcí a to detekci hrozeb (IDS) a jejich prevenci (IPS). Dokáže tak pracovat díky hloubkovému procházení paketů, což je pro detekci hrozeb a útoku primární. Dokáže provádět detekci narušení v reálném čase, online prevenci narušení, offline *pcap processing* a monitorování zabezpečení sítě. I když je Suricata velice podobná systému Snort, má oproti němu značné výhody. Jedná se o vícevláknový software, takže jedna instance může fungovat při značně vyšších objemech provozu. Nabízí větší podporu pro protokoly aplikační vrstvy. To znamená, že dokáže identifikovat některé z běžnějších protokolů aplikační vrstvy např. TLS, HTTP, kdyby využívali ke komunikaci nestandardní port. Podporuje však i sledovaní aktivity na nižších úrovních např. TCP, UDP, ICMP, IP. Podporuje také hašovaní a extrakci souborů. Má podporu skriptovacího jazyka Lua, který lze použít k úpravě výstupu, či k vytváření komplexní logiky u detekce podpisů služeb. Suricata podporuje všechny standardní výstupní a vstupní formáty a lze jí snadno integrovat do jiných databází. [18, 19]

Využívá dva různé typy pravidel a to soubor pravidel od společnosti ETPro, kteří nabízí také jejich neplacenou verzi ETCommunity. Za zmínku také stojí říct, že již obsahuje více než 47 000 pravidel. Další možností pravidel jsou pravidla od společnosti Snort a to jak pravidla placená, tak ta zdarma.

Značnou výhodou je možnost správy Suricaty v GUI, pokud infrastruktura využívá pro správu sítě software pfSense. Ten nabízí IDS Suricata jako plugin, který lze přidat do softwaru. Poté lze veškeré věci řešit v grafickém rozhraní. Nabízí zde výpis upozornění, možnost zobrazení důležitých logů, přidávaní nových rozhraní apod..

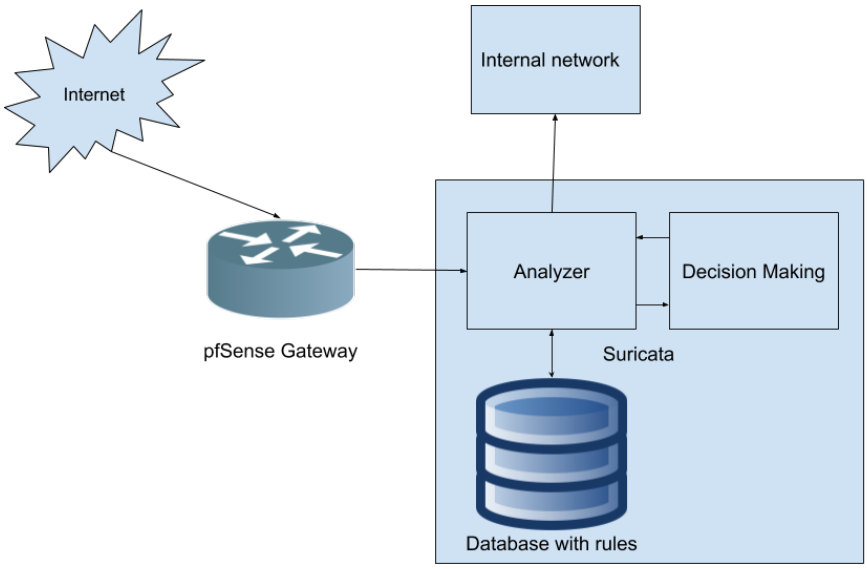
Díky inteligentní architektuře zpracování, využívá vícevláknové činnosti, což urychluje hardware. Jedná se o velmi vítanou funkci, jelikož Suricata může být tzv. *heavy on processing*.

Na obrázku číslo 4.2 lze vidět architekturu systému Suricata s využitím softwaru pfSense. Paket, který dorazí z internetu se zastaví na bráně pfSense. Odtud jej pošle právě do Suricaty, kde se buď vytvoří upozornění na daný paket a zablokuje jej, pokud je tak systém nastaven, nebo jej pošle dále do systému, kde se doručí do cíle.

Mezi hlavní výhody Suricaty určitě patří škálovatelnost, díky využívání více vláken. Skvěle kooperuje se softwarem pfSense, který mu nabízí decentní grafické rozhraní, které práci s nastavením této služby usnadňují. Patří mezi nejvyužívanější open-source IDS nástroje a existuje mnoho různých modifikací vytvořené komunitou. Nabízí se také propojení s monitorovacím softwarem Grafana, které umožní grafické zobrazení záznamů aktivit. [19, 18]

4.1.4 Snort

Snort je na trhu řadu let. Ačkoliv nepatří mezi první IDS nástroje, řadí se k těm nejdéle používaným. Snort se řadí mezi open-source IDS softwary, řadu let měl svou komerční verzi Firepower. Tento



Obrázek 4.2: Architektura softwaru Suricata v propojení se softwarem pfSense

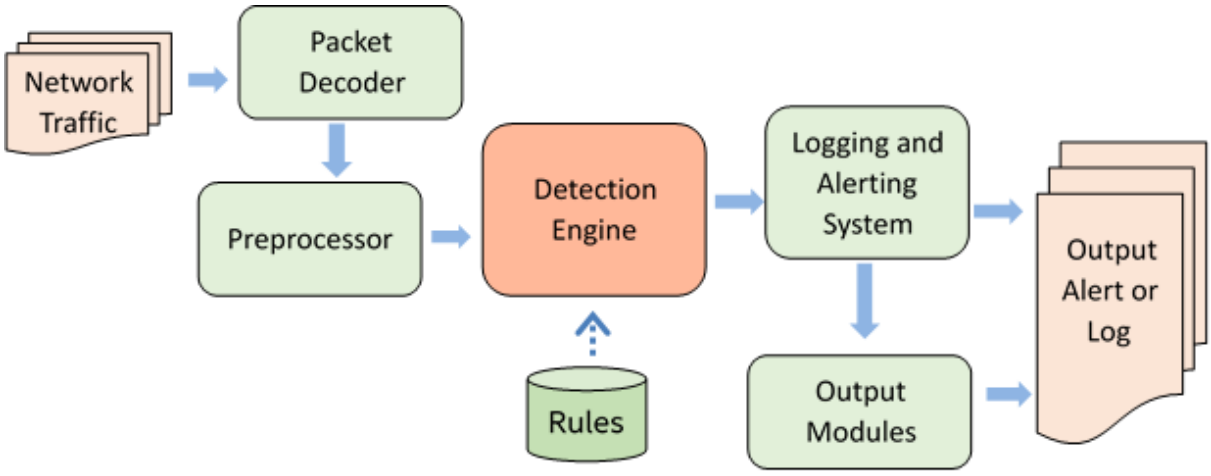
software v roce 2013 odkoupila firma Cisco. Snort byl vytvořen programátorem Martinem Roeschem v roce 1999.

Snort je velmi konfigurovatelný a lze jej provozovat na více operačních systémech či hardwarových platformách. Software se nechtěl spoléhat na knihovnu libpcap, a proto zavedl novou vrstvu DAQ (Data Acquisition). DAQ poskytuje abstrakci pro prostředky pro zpracovaní paketů, která je odděluje od používání knihovny libpcap, tudíž je možné využít jiné knihovny, v závislosti na jaké platformě je Snort nainstalován. Libpcap je multiplatformní knihovna, která poskytuje API rozhraní pro příjem paketů přímo ze sítě.

Snort měl během svého působení řadu přispěvatelů, kteří přidali spoustu funkcí. Software tedy obsahuje spoustu konfigurovatelnosti a řadu externích funkcí, jednou z nich jsou preprocesory. Zkušení programátoři mohou vytvářet vlastní preprocesory a začít je v Snortu využívat. Preprocesory se spouští po dekódování paketu, ještě před zpracováním pravidel. Snort zpracovává pakety, avšak pakety nemusí obsahovat celou zprávu, a pokud by detekce závisela pouze na kontrole paketů, mohl by jí útočník snadno obejít. Z toho důvodu je možné využít právě jeden z preprocesorů nabízený Snortem, který se zabývá rekonstrukcí TCP streamu. Protože zpráva se může skládat s několika paketů a jejich posílaní běží v TCP streamu. [18, 20]

Na obrázku číslo 4.3 můžete vidět architekturu nástroje Snort. Jak již bylo popsáno, prvně se paket dekóduje a následně dojde k zpracovaní preprocesorů. Jakmile jsou načteny všechny preprocesory, dochází k předání dekódovaného paketu do detekční části, která se dotáže na sadu pravidel nastavených administrátorem. Výsledkem je vygenerovaná zpráva, případně upozorní systém na vzniklou nesrovnalost.[21]

Software neobsahuje základní grafické rozhraní a veškeré ovládání se provádí pomocí konzole,



Obrázek 4.3: Architektura IDS od společnosti Snort [21]

která může být pro nové uživatele celkem náročná. Existují však různé nástroje, které poskytují pro Snort IDS webové rozhraní pro dotazování a analýzu upozornění. Systém využívá tzv. modulární design, který rozděluje systém na menší moduly, které lze nezávisle vytvářet, upravovat, nebo nahrazovat. Využívá vícevláknové zpracování paketů. Obsahuje také analyzátor pravidel a syntaxí. Dále nabízí služby pro automatickou detekci pro konfiguraci bez portů. Společnost také nabízí předem vytvořená pravidla, která nabízí buď v bezplatné verzi, nebo jejich placená pravidla, která jsou pravidelně aktualizována. Tyto pravidla je možné stáhnout z jejich oficiálních webových stránek.

Výhodou využívání IDS od společnosti Snort je možnost konfigurace všech jeho funkcí, pravidel, přidávání vlastních či již vytvořených externích preprocesorů. Tím jak je na trhu delší dobu, má velkou podporu komunity a systém je důkladně prověřený a testovaný. Nabízí jak neplacená tak placená pravidla. Mezi nevýhody patří chybějící grafické rozhraní, které by napomohlo snadnější konfiguraci a přehlednějšímu zobrazení zaznamenaných upozornění. [18, 20]

4.1.5 Komerční IDS řešení

První nástroj, který je zde uveden, je SolarWinds Security Event Manager. Jedná se o komerční software, který nabízí třiceti denní zkušební verzi. Cena za tento nástroj začíná okolo 4000$ ročně. Využívá vysoce inteligentní přístup k detekci hrozeb. Shromažďuje informace o typech a množství útoků. Tyto informace jsou integrovány do dalších protokolů, které napomáhají k detekci dalších potencionálních hrozeb.

Využívá nativní technologii, díky ní nemusí technik provádět rutinní úkoly např. sledování a upozorňování na jakékoliv podezřelé události, provádí také analýzu dat. To je jen krátký výpis, co vše dokáže tento software nabídnout. Má sofistikovaný systém upozornění. Lze přiřadit jednotlivé práva pro každého uživatele. Přestože obsahuje velice pokročilé nástroje, je uživatelsky velice pří-

větivý a není nutné strávit několik desítek dnů, aby nový administrátor pochopil všechny nabízené funkce. Data jsou prezentována graficky, jsou tak snadno čitelná. Tento software je k dispozici pro všechny standardní operační systémy jako je Windows, Linux nebo MacOS.[22]

Dalším komerčním nástrojem je CrowdStrike Falcon. Software nabízí patnácti denní zkušební verzi. CrowdStrike Falcon je spíše host-based detekční systém, protože se zabývá ochranou koncových bodů. Nejedná se však o typický HIDS, nezaměřuje se totiž přímo na protokolové soubory na monitorovaném zařízení, ale zkoumá procesy běžící na všech spuštěných zařízeních.

Platforma Falcon je řízena pomocí balíčků modulů. Obsahuje dva hlavní moduly. Prvním je Falcon Insight, který poskytuje funkce HIDS, detekci koncových bodů a reakce na hrozbu. Dále tento modul hledá systémová narušení. Druhým modulem je Falcon Prevent. Jeho jádrový modul je EPP(Endpoint protection), ten využívá metodiky k detekci škodlivého chování a hledá škodlivé softwary, které mohou běžet na pozadí připojeného stroje. Rozdíl mezi těmito moduly je malý, jelikož každý sleduje anomálie v běhu systému. Zaznamenávají události do souborového protokolu. CrowdStrike využívá agenty, který komunikuje s centrálním systémem pro zpracování, který je rezidentem v cloudu. Technik ovládá software pomocí jakéhokoliv standardního prohlížeče. Výhodou této hybridní architektury je nízký nárok na hardware zařízení. Veškerý výpočetní výkon je dodáván analytickým softwarem na serverech CrowdStrike. [23]

4.1.6 Shrnutí IDS nástrojů

Celá tato kapitola se zabývala podrobným rozborem IDS nástrojů, převážně těch open-sourcových. Právě cena je hlavním parametrem pro implementaci IDS nástroje pro tuto infrastrukturu. Funkcionalita obou komerčních nástrojů je velmi pestrá, ale jejich provoz je velice nákladný. Nejlepší volbou IDS nástroje je Suricata. Tento nástroj splňuje veškeré požadavky na IDS software. Výhodou je možné propojení se softwarem Suricata, jak bylo zmíněno v kapitole 4.1.3 o Suricatě a dokáže využívat soubory pravidel i od IDS nástroje Snort. Instalace a konfigurace tohoto nástroje je popsána v následujících kapitolách.

4.2 Skenování a správa zranitelnosti

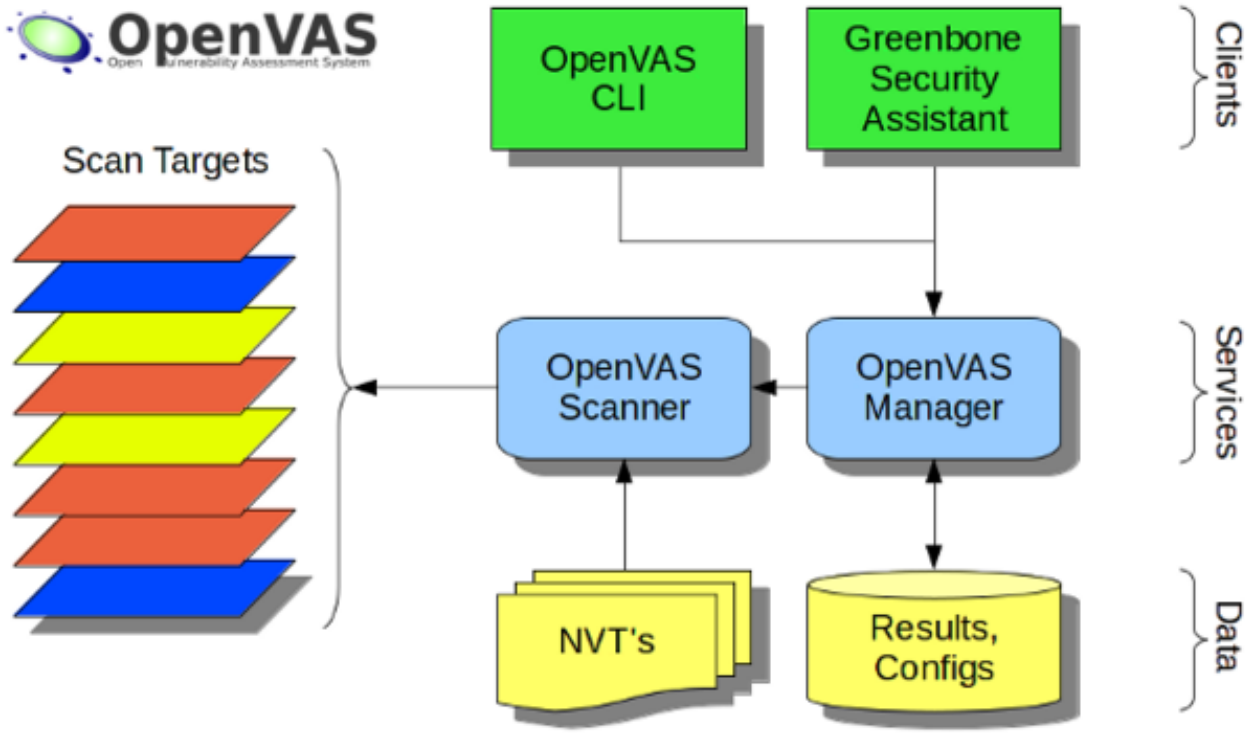
Správa zranitelnosti se stará o identifikaci, hodnocení a hlášení zranitelnosti v systémech a softwaru na kterých běží. Skenování a správa zranitelnosti, která je implementovaná společně s dalšími bezpečnostními systémy, je zásadní pro stanovení možných hrozeb a minimalizaci možného místa napadení.

Na trhu je velké množství nástrojů, které se zabývají správou zranitelnosti. Existují jak v open-source verzích, tak komerčních. Mezi oblíbené nástroje se řadí open-source nástroj OpenVAS, nebo

komerční nástroj Nessus. Dalšími známými programy na trhu jsou Netsparker, Nmap, Aircrack, SolarWinds Network Configuration Manager a mnoho dalších.

4.2.1 OpenVAS

OpenVAS patří k nástrojům, které se zabývají skenováním zranitelností v síti. Software je vyvíjen firmou Greenbone Networks od roku 2009. Jedná se o plně bezplatný software. OpenVAS dokáže provádět ověřená, tak i neověřená testování. Dále provádí mnoho vysoko a nízko úrovňových úloh, které se týkají průmyslových a internetových protokolů. Obsahuje interní programovací jazyk pro implementaci jakýchkoliv typů testů. Systém nabízí různé nástroje pro nastavení sofistikovanějšího testování. [24]



Obrázek 4.4: Architektura systému OpenVAS [25]

Na obrázku číslo 4.4 vidíme strukturu softwaru, která bude v následující části rozebrána. Architektura se dělí do tří částí.

- První jsou klienti. OpenVAS CLI je konzole nabízená tímto software, pomocí které můžeme ovládat všechny prvky. Dále také OpenVAS obsahuje grafické rozhraní, které je součástí Greenbone Security Assistant. Jedná se o webové rozhraní, které nabízí grafy výstupních dat, výsledky testů apod.

- Druhou částí jsou služby, které jsou hlavní částí celého softwaru. OpenVAS Manager dostává příkazy od klientů přes OpenVAS Management protokol. Tento protokol byl navržen a implementován Greenbone Networks. Manager se poté dotazuje databáze, kde jsou uloženy např. nastavení cílů, výsledky testů, aby mohl splnit zadaný příkaz. OpenVAS Scanner je hlavní částí pro skenování sítě. Komunikace mezi skenerem a manažerem probíhá pomocí OpenVAS Transfer protokolu.

- Poslední částí jsou data. Skener pracuje s databází NVT(Network Vulnerability Test). Tato databáze je pravidelně aktualizována a obsahuje téměř 53 000 testů, kterými můžete otestovat zranitelnost vaší infrastruktury. Skener následně otestuje vybrané cíle a výsledek uloží do databáze.

OpenVAS nabízí řadu funkcí, pomocí kterých můžeme skenování zranitelností automatizovat. Nabízí možnost takzvaného sofistikovaného skenování. Je možné nastavit plánovače, odesílat oznámení na e-mail, nastavit skenování jednoho počítače či celé sítě a mnoho dalších užitečných funkcí.

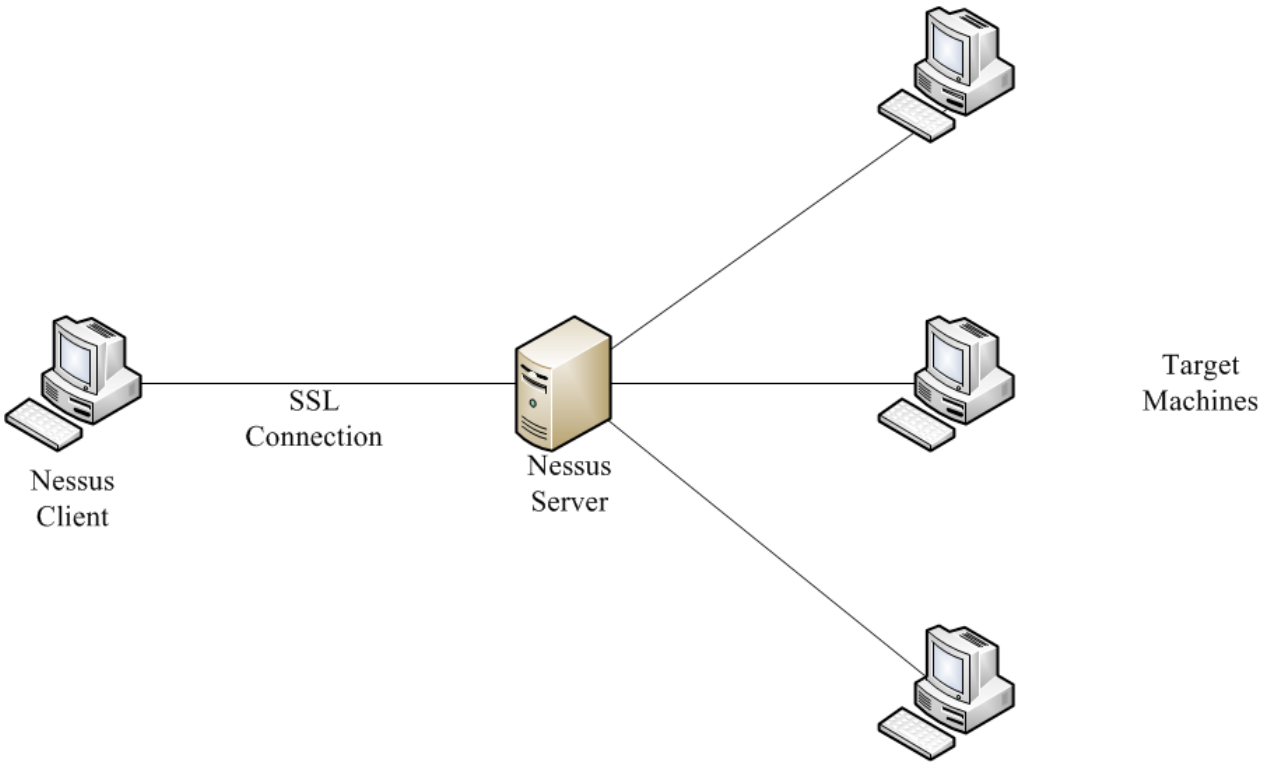
Výhodou tohoto nástroje je možnost si naprogramovat vlastní typ testovacích funkcí. Nástroj je kompletně bezplatný, tudíž uživatelé neztrácí funkcionalitu jako u jiných nástrojů. Vývojáři připravili přehledný manuál pro uživatele, aby mohli využít přednastavené funkce. Nevýhodou je méně kvalitní grafické rozhraní, co se u open-source nástrojů dá očekávat. Avšak i toto grafické rozhraní je dostačující pro práci s tímto softwarem. [26, 27, 24]

4.2.2 Nessus

Software vyvíjený firmou Teneble, Inc.. Multiplatformní nástroj pro nejpoužívanější operační systémy, jako jsou Linux, Windows nebo Mac. Pokrývá celou řadu technologií včetně operačních systémů, síťových zařízení, hypervizorů, databází, webových serverů a kritické infrastruktury.

Nástroj se skládá z klienta a serveru viz obrázek číslo 4.5. Klient obsahuje webové rozhraní, které mu umožní ovládat veškeré funkce z jednoho místa bez nutnosti větších znalostí příkazů pro spouštění skeneru. Server komunikuje s databází, kde jsou uloženy testy. Komunikace mezi klientem a serverem probíhá pomocí SSL připojení.

Skenování lze automatizovat v unixovém systému pomocí příkazové řádky, nebo pomocí nastavení ve webovém rozhraní. Při vytváření nového sledování si můžete vybrat z řady specifikovaných testů např. Malware Scan, Basic Network Scan, Host Discovery a mnoho dalších. Výsledky z testů je možné anonymně přidávat do již obsáhlé databáze znalostí. Díky této databázi můžeme jednoduše nalézt odpovědi, jak opravit nalezené chyby, které již byly do databáze znalostí přidány dříve. Nessus obsahuje také funkci Live Scan. To umožní administrátorovi sledovat průběh v realném čase. Nástroj také obsahuje možnost správy mobilních zařízení. Díky této funkci můžete udržovat mobilní zařízení vaší společnosti aktualizovaná a snížíte tak možnosti napadaní. Nástroj nabízí přehledná hlášení o výsledcích testů. Jsou interaktivní, tudíž je možné se v nich snadno zorientovat. [29, 30]



Obrázek 4.5: Architektura nástroje Nessus [28]

Nessus je odstrašující svou vysokou cenou, proto se nedá dobře uplatnit v malých projektech. Hlavní výhodou je přehledný výpis hlášení, které může být bez úprav použito pro poskytnutí bezpečnostních auditů na týmových poradách. Má velice intuitivní uživatelské rozhraní, jednoduché nastavení sofistikovanějšího testování a další. Základní balíček funkcí lze pořídit zdarma. Jedná se o produkt Nessus Essentials. Nabízí všechny základní funkce pro skenování zranitelnosti. Hlavní nevýhodou je počet nastavených testování, který je velmi limitující, tudíž se dá použít spíše v domácím prostředí.

4.2.3 Srovnání nástrojů

Tyto dva nástroje byly vyvíjeny stejnými programátory, kteří se po koupi společnosti rozdělili na dva tábory. Jedna část pokračovala ve vyvíjení Nessus, druhá vytvořila software OpenVAS. Softwary jsou si velmi podobné, ale liší se v mnoha aspektech.

Jelikož je Nessus komerčním nástrojem oproti OpenVAS, na vyvíjení aplikace jsou použity větší finanční prostředky. Z tohoto důvodu se výrazně liší jejich grafické rozhraní. Grafické rozhraní od společnosti Nessus je uživatelsky přívětivější oproti grafickému rozhraní od společnosti OpenVAS. V Nessusu je všechno potřebné nastavení na jednom místě oproti systému OpenVAS, který má nastavení rozdělené. Další rozdílem je počet přednastavených typů skenování. Nessus obsahuje mnohem více již vytvořených funkcí pro odlišné testovací účely.

Pro běžného uživatele, který chce zabezpečit svou malou síť do pěti zařízení, je skvělá volba Nessus Essentials. Pro větší organizace s velkým rozpočtem do oblasti zabezpečení je dobrá volba software Nessus Professional. Výhodou je velká podpora a rozvoj softwaru. Nabízí mnoho funkcí na hodně vysoké úrovni. Pro ostatní je skvělým východiskem software OpenVAS, který dokáže skvěle zastoupit své komerční konkurenty. Menším organizacím ušetří finance na úkor delšího učení obsluhy softwaru a využití jeho funkcí.

Na základě těchto faktů, byl zvolen software OpenVAS, který pro tuto síťovou infrastrukturu plně vyhovuje a bude poskytovat dostatečné informace o zabezpečení sítě.

Kapitola 5

Automatizace

S rostoucí společností či firmou se v přímé úměře zvětšuje i jejich IT infrastruktura. Důsledkem toho vzniká více pracovních procesů, které se postupem času bez automatizace nedají stihnout dodělat včas. Proces je v podstatě odkaz na řadu úkolů, které se musí provést, aby se docílilo požadovaného výsledku. Je tedy nutné se zamýšlet nad problematikou automatizace, aby došlo ke zrychlení řešení těchto základních úkonů. Procesy lze automatizovat na různých úrovních. Hlavním rozdílem mezi úrovněmi spočívá v tom, zda proces řídí člověk, zda proces řídí počítač, nebo je proces plně automatizovaný. Dále se automatizace může dělit do dvou kategorií a to automatizaci samotných úkolů, nebo automatizace toku řízení mezi úkoly.

- Automatizace úkolů - tyto úkoly jsou zpracovány automaticky např. za pomoci nějakého softwaru či robota.
- Automatizace toku řízení - interakce mezi úkoly jsou zautomatizovány, ale samotné úkoly jsou vykonávány člověkem.

Tyto metody lze kombinovat a tím docílíme plně automatizovaných procesů, v angličtině známe jako *straight-through processing*(STP). Tyto procesy potřebují lidský zásah jen tehdy, kdy se stane něco nad očekávání běžného provozu. [31]

5.1 Automatizace infrastruktury

Úvod této kapitoly se vztahoval k obecné automatizaci. Tato podkapitola je zaměřena na důležitost automatizace pracovních procesů v rozsáhlejší infrastruktuře. Cílem automatizace infrastruktury je využívat různé technologie, které provádí úkoly se sníženou nutností obsluhy za účelem řízení hardwaru, softwaru a síťových komponentů. S omezeným počtem zaměstnanců dochází k prodlevám u aktualizací softwaru, přidávaní nových aplikací. Při těchto prodlevách dochází k bezpečnostnímu riziku, jelikož stroje nejsou aktualizované a útočníci by mohli využít chyb z předchozích verzí aplikací, či operačního systému. Užití automatizačních softwarů na provádění běžných úkonů ušetří

správcům infrastruktury hodně času a jejich zaměstnavatelům peníze. Díky automatizaci dochází také ke snížení výskytu možných chyb, které jsou způsobeny lidským faktorem. [4]

V následujících podkapitolách popíšu nejpoužívanější softwary, které se zabývají automatizovanou správou infrastruktury, nebo napomáhají s řízením a nastavováním nových komponentů v infrastruktuře.

5.1.1 Ansible

Software Ansible původně vyvinul programátor Michael DeHaan, který je také autorem softwaru Cobbler, který byl vyvinut během jeho působení v Red Hat. Cobbler je instalační Linux server, který umožňuje rychlé nasazení serverů v síti. Pomáhá s nastavením DNS, DHCP, aktualizacemi a distribucí balíčku, nasazením virtuálních strojů a přidáním jak fyzických tak virtuálních strojů do systému správy konfigurace. V únoru roku 2012 DeHaan se zavázal k projektu Ansible a ve vydaném `README` uvedl jednoduchý popis, čím vlastně Ansible bude. Tato zpráva vzbudila velký zájem, a proto v roce 2013 vznikla firma Ansible Inc.. Poslední velkou událostí bylo odkoupení této společnosti firmou Red Hat. To bylo v roce 2015 a od té doby se podílí na vývoji tohoto softwaru. [32]

Ansible je software pro správu konfigurace, který běží na jednoduchém rozhraní Python API. Nevyžaduje žádný řídící stroj, kde by začínala orchestrace. Ansible obsahuje inventář, ve kterém jsou uloženy jeho konfigurace. Inventář může být nahrán lokálně, nebo jej můžeme stahovat z dynamických či cloudových zdrojů. Typickým formátem souboru je soubor s příponou YAML. Uzly jsou spravovány obvykle řídícím strojem pomocí protokolu SSH. [33]

Při porovnání prvního vydání s aktuální verzí Ansiblu, je z prvního pohledu jasné, že došlo k mnoha úpravám a dodatkům. Základní princip však zůstává stejný. Tyto principy budou teď uvedeny.

- **Bez Agentů** Všechna správa je řízena pomocí protokolu SSH, u počítačů s operačním systémem Windows pomocí protokolu WinPR. Nemělo by se spoléhat na vlastní agenty nebo nestandardní porty, které je nutné cílovým zařízením povolit, nebo s nimi pracovat.

- **Minimalistický** Schopnost spravování nových vzdálených počítačů, bez nutnosti instalace jakýchkoliv balíčku či softwarů, protože každá minimalistická instalace Linuxu obsahuje balíčky pro SSH a Python.

- **Jednoduchý** Klade se důraz na jednoduché a intuitivní tvoření nových Playbooků a jejich případné konfigurace.

- **Snadné použití** Snaží se být nejjednodušším IT systémem, který slouží pro automatizaci.

Těmito kroky se právě liší od svých podobných nástrojů jako je Puppet nebo Chef. [32]

5.1.2 Citrix

Citrix je americká nadnárodní společnost, která poskytuje řadu služeb jako jsou virtualizace serverů, aplikací, sítí nebo cloudové služby. Společnost byla založena v roce 1989 v Texasu, V počátcích se zabývala vývojem produktů pro vzdálený přístup k operačním systémům od společnosti Microsoft. Citrix se také proslavil jako lídr ve vývoji *Thin Client*. Postupem času expandovali do dalších odvětví: virtualizací serverů, desktopů a cloudových služeb. [34]

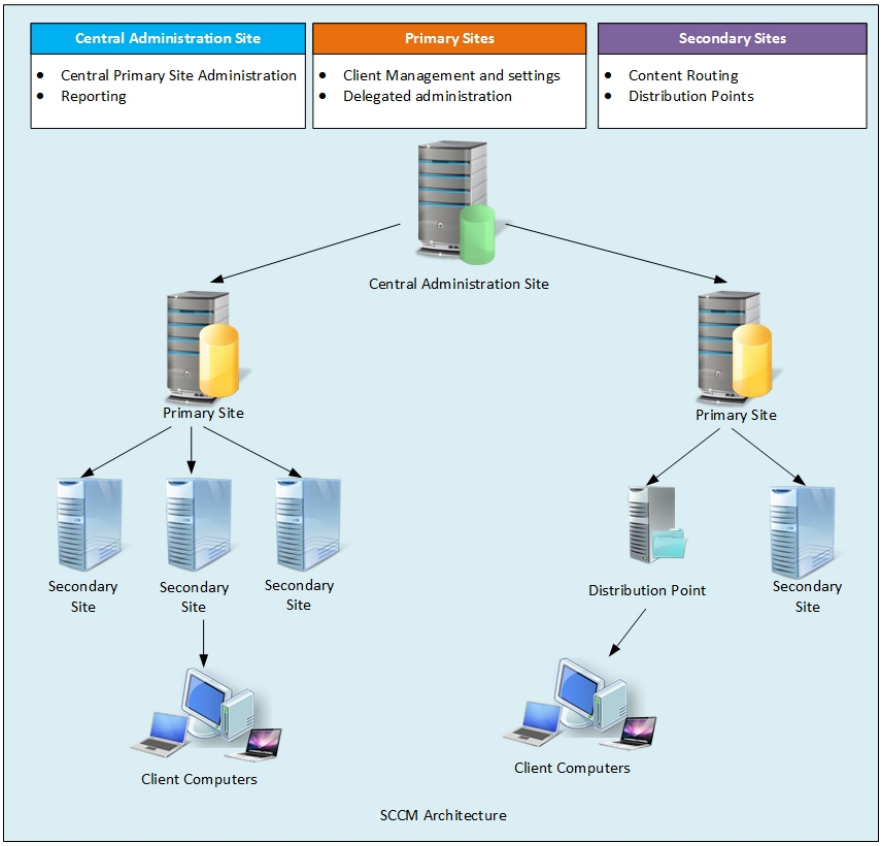
První z řady produktů Citrix je software Citrix Workspace. Jedná se o kompletní digitální řešení pracovního prostoru, který umožňuje poskytování zabezpečeného přístupu k aplikacím, informacím, případně přístupu k dalším informacím, které odpovídají relevantní roli zastupující v organizaci. Software pomáhá s organizací a automatizací klíčových informací, které uživatelé potřebují ke spolupráci. Program obsahuje funkci pro usnadnění vyhledávání, kde dokáže nalézt relevantní informace ze všech souborů a aplikací. Výhodou softwaru je uchovávat všechny potřebné informace na jednom místě. Tudíž je zde výrazně menší pokles počtu nutnosti přihlášení. I tato triviální záležitost uleví správcům infrastruktury, protože dochází k poklesu zasílání ticketů na zapomenutá hesla. Využívá funkce virtuální asistence, která automatizuje opakující se úkony. Citrix Workspace poskytuje pracovní prostor pro všechny technologické vrstvy. Řešení slouží ke správě koncových zařízení, řízení přístupu, řízení virtuálních aplikací a pracovní plochy. Produkt nabízí ve čtyřech variantách a jak je již zvykem, každá dražší varianta obsahuje více funkcí a vyšší podporu od vývojářů. Tento software využívá řada úspěšných společností po celém světě, mezi které například patří ABB, UnicreditBank, Intel, NASA a spousta dalších. [35]

5.1.3 System Center Configuration Manager

Software vyvinut společností Microsoft v roce 1994, tehdy veden pod názvem Systems Management Server. Do stávající podoby se dostal v roce 2007. Od této doby se výrazně neměnila funkčnost samotného systému. Byly vydávány pouze rozšiřující aktualizace, které odpovídaly aktuálním operačním systémům a umožňovaly spravovat jejich nové funkce prostřednictvím tohoto nástroje. Konfigurační manažer je placené řešení pro správu produktů od společnosti Microsoft. Dokáže sledovat inventář sítě, pomáhá s distribucí aplikací a nasazuje aktualizace a opravy operačních systému a programů v celé síti. Díky těmto funkcím je atraktivním softwarem pro velké podnikové firmy, které potřebují řešit správu více fyzických i virtuálních počítačů v síti.

Konfigurační manažer potřebuje pro svou instalaci minimálně dva Windows servery. První server bude zastávat roli DHCP, DNS a Active Directory serveru, který bude naplněn informacemi o celé síti. Druhým serverem bude primární Site server, který bude pracovat jako konfigurační manažer. Primární Site server dokáže zastávat role Management Point, Software Update Point, Distribution Point a další. Konfigurační manažer může spolupracovat s dalšími sekundárními Site servery, které budou spravovat určité role konfiguračního manažera. Tato funkce nalezne uplatnění pouze u velkých společností, které potřebují rozdělit svá zařízení mezi více serverů z důvodu zahlcení primárního

Site Serveru. Konfigurační manažer potřebuje k ukládání získaných dat SQL server. SQL server může být instalován lokálně na primárním Site serveru, nebo může být veden jako vlastní server. Lokální řešení je mnohem jednodušší, a pokud počet klientů nedosahuje maxima lokálního SQL serveru, není nutné řešit složitější variantu. Právě SQL server přidává hardwarové požadavky pro plynulý běh konfiguračního manažera. Minimální operační paměť pro běh lokálního SQL serveru je 16GB, a to 8GB je rezervováno pro SQL server a 8GB pro Site server. Primární server musí mít přidaná dostatečná práva, aby mohl získávat informace z Active Directory o zařízeních a uživatelích v síti. Na obrázku číslo 5.1 je vidět možná architektura konfiguračního manažera pro rozsáhlejší infrastrukturu. [36]



Obrázek 5.1: Architektura SCCM [37]

Jak jsem již zmínil, konfigurační manažer usnadňuje správu zařízení v síti. Konfigurační manažer zahrnuje širokou škálu funkcí, které poskytují určitou flexibilitu. Poskytuje také řadu nástrojů pro zabezpečení koncových bodů a se správnou konfigurací může být jediným systémem pro celou správu podnikové sítě. Jako produkt společnosti Microsoft nemá problém se zavedením ostatních produktů od této společnosti do konfiguračního manažera. V posledních letech se snaží přizpůsobit trendu připojení zařízení používané zaměstnanci tzn. správa koncových bodů. Správa se řídí pomocí uživatelského grafického rozhraní. Nástroj má velkou komunitní podporu a také podporu od

samotného Microsoftu.

Nevýhodou tohoto nástroje je jeho cena. Nástroj SCCM je většinou součástí větší sady nástrojů od společnosti Microsoft. Také požadavky na server, který je určen právě pro SCCM nejsou nejmenší. Musí obsahovat dostatek operační paměti, aby dokázal utáhnout samotný konfigurační manažer, ale také SQL server, který je pro tento software stěžejní. Konfigurační manažer nedokáže poskytnout stejné funkce pro správu ostatním operačním systémům. Operační systémy jako jsou Linux či MacOS mohou být v SCCM vedeny pouze jako zařízení koncových klientů. Omezená je taky správa a možnost aktualizace softwarů třetích stran.

Jedná se o komplexní nástroj, který je zaměřen výhradně na produkty společnosti Microsoft. Jeho využití není tak rozšířené jako u ostatních nástrojů, jelikož mnoho společností v dnešní době využívá v infrastrukturách zařízení s různými operačními systémy. [38]

Kapitola 6

Instalace a konfigurace nástrojů pro bezpečnostní audity

Po provedeném rozboru nástrojů, které slouží pro hlídání síťového provozu a vytváření bezpečnostních auditů, byly vybrány dva nástroje. Prvním nástrojem je software OpenVAS, který provádí skenování vytvořených cílů a sbírá informace o potencionální zranitelnosti. Druhým nástrojem je Suricata, která slouží jako IDS. Kapitola je zaměřena na popis instalace a konfigurace těchto nástrojů, aby bylo docíleno získávání pravidelných auditů.

6.1 Instalace OpenVAS

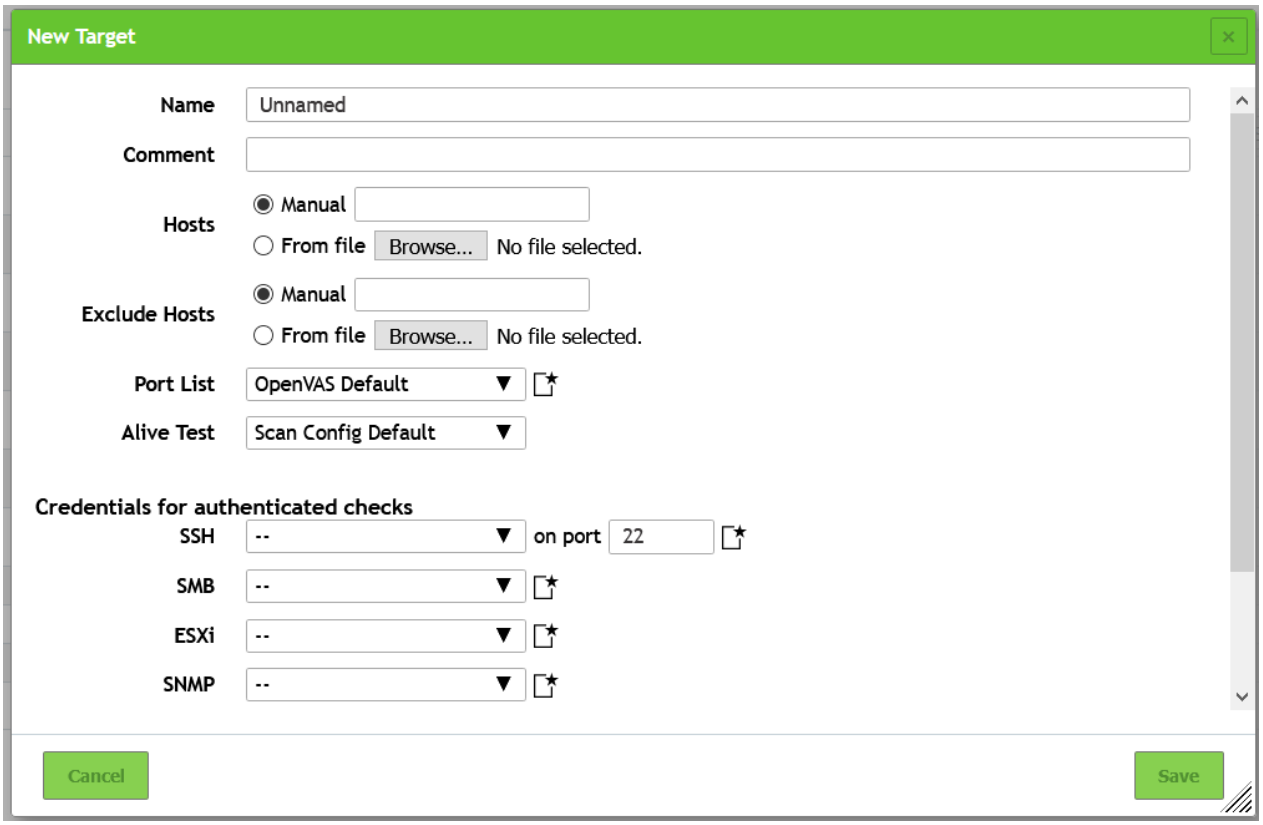
Instalace softwaru OpenVAS byla provedena na operačním systému Centos 7. Prvním krokem bylo zakázaní funkce SELinux. SELinux je rozšíření jádra Linuxu, které slouží k zvýšení počítačové bezpečnosti. Bylo nutné provést povolení portu 9392, na kterém běží webové rozhraní pro OpenVAS. Bylo potřeba přidat repozitář, který obsahoval yum balíček. Samotná instalace byla provedena pomocí yum balíčku. Při instalaci bylo nutné vyplnit uživatelské jméno a heslo pro administrátora. Tímto účtem se pak přihlašuje ve webovém rozhraní. Po dokončení instalace se spustí služba OpenVAS a zkontroluje se, zda-li v pořádku běží. Pro přístup ke konfiguraci je použit webový prohlížeč a na adrese `https://openvas.domena:9392/` se provedlo přihlášení a začalo se s konfigurací nástroje.

6.2 Konfigurace OpenVAS

Aby bylo docíleno sofistikované kontroly zranitelnosti, je důležité nastavit řadu funkcí: cíle, plánovač, upozornění. Pro spuštění jednorázového testu není nutné tyto části nastavovat. Je možné vyvolat spuštění testu přímo v sekci *Scans/Tasks* a zde je vytvářena nová úloha.

6.2.1 Nastavení cílů kontroly zranitelnosti

Nastavení cílů se nachází v záložce *Configurations/Targets*. V levé horní části je zobrazena ikona s názvem *New Target*. Po kliknutí se objeví nové okno, ve kterém lze nastavit vše potřebné pro daný cíl. Jako první bylo nastaveno jméno, pod kterým se bude zobrazovat při vytváření skenování. Poté bylo stanoveno, na které stroje se má cíl vztahovat. Je možné přidat IP adresu pouze jednoho stroje, nebo výběr IP adres či celou síť. Dalšími parametry jsou *Port List, Live test*. Pro nastavení Port listu bylo použito základní nastavení portů od OpenVAS, kde jsou vybrané nejpoužívanější TCP a UDP porty, jako jsou FTP, HTTP, SSH, Telnet a další. Je možnost přidat vytvořená pověření pro ověřené kontroly, které se dají využít v hloubkovém skenování. Vytváření těchto cílů umožňuje jednoduše nastavovat skenery. Není nutné znát dané IP adresy, neboť pomocí přiřazených názvů lze nastavit pro daný cíl jakýkoliv typ skenu. Zde byly vytvořeny cíle, které pokryly většinu sítě. Na obrázku číslo 6.1 můžete vidět, jak okno pro vytvoření nového cíle vypadá.



Obrázek 6.1: Vytvoření nového cíle

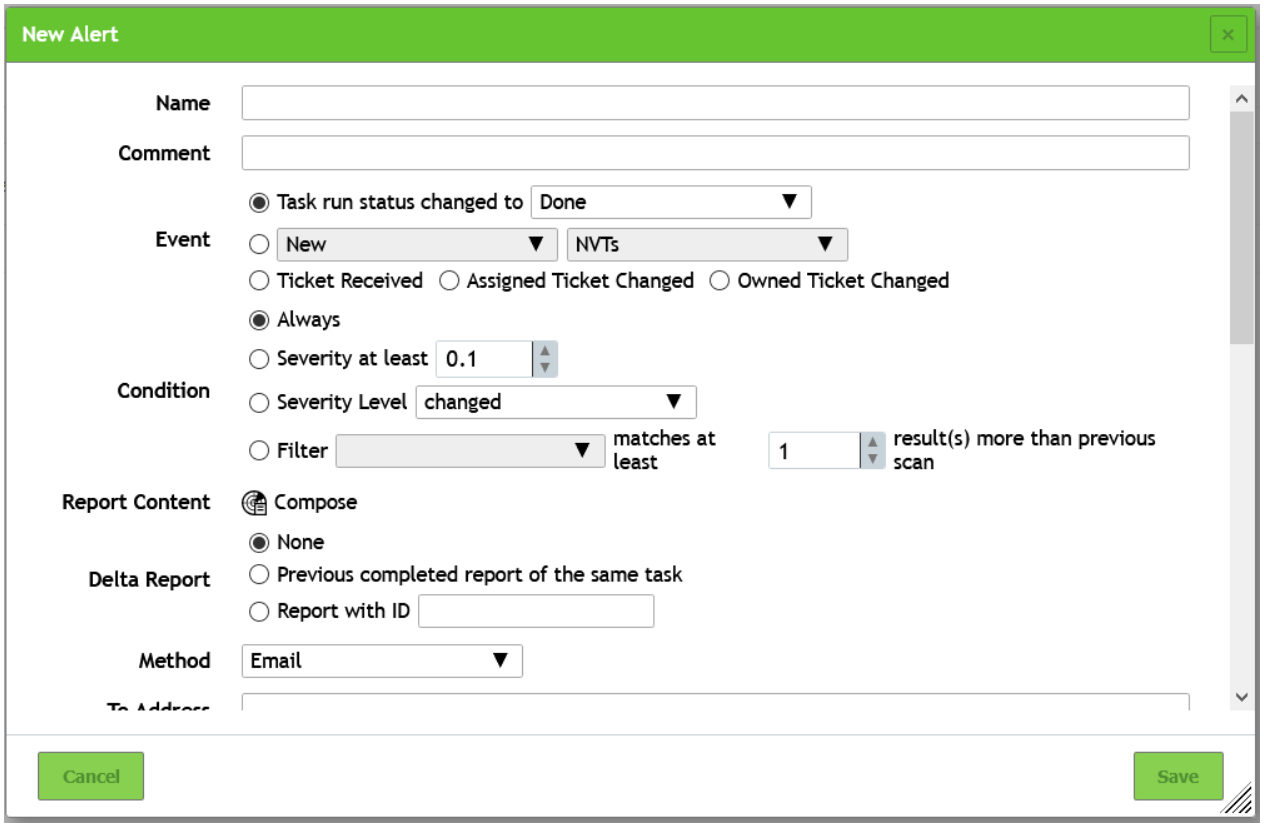
6.2.2 Nastavení plánovače

Aby se průběh skenování automatizoval, bylo nutné nastavit plánovač, kdy se dané testy mají provádět. Byly vybrány tři různé časové doby, aby se rozvrhlo zatížení na server. První testování je

naplánováno na 22:30 a další jsou od něj vzdáleny v hodinu a půl dlouhých intervalech. V jednom intervalu se spustí 5 až 7 skenů, které stihnou za tu dobu dokončit všechny úkoly. Rozdělení bylo použito z důvodu větší bezpečnosti. Mohlo by dojít například k nečekanému výpadku v důsledku testování, proto není bezpečné testovat hlavní i záložní server v jeden čas, na kterém běží například Active Directory.

6.2.3 Vytváření upozornění

Dojde-li k nějaké změně, která je pro správce důležitá, dostane upozornění například v podobě e-mailu. Nastavení upozornění se nachází v záložce *Configurations/Alerts*. Zde se nachází výpis již vytvořených pravidel, která můžeme upravovat či vytvořit nová. Základem je určit, co je pro správce důležitá změna, která zašle upozornění. První pravidlo pro odeslání upozornění je, když dojde ke změně vážnosti (severity) po vykonaném skenu. Toto pravidlo bylo aplikováno u každého standardně nastaveného skenu. Výhodou tohoto typu upozornění je nízká nutnost pravidelných kontrol hlášení. Pokud správce nedostane upozornění, nedošlo od minulého skenu k žádné změně. Dalšími pravidly, které je možno nastavit, jsou zvýšení vážnosti na určitou úroveň, nebo zasílání zpráv po každém dokončení. Na obrázku 6.2 je vidět okno, ve kterém se provádí konfigurace upozornění.



Obrázek 6.2: Vytvoření upozornění

Pro odesílaní upozornění je možné vybírat z řady metod, které jsou v OpenVAS implementovány. Zde je pár příkladů:

- System Logger
- HTTP GET
- SCP
- Email

Pro odesílání zpráv byla vybrána možnost pomocí emailu. Zprávy budou odesílány na SMTP server, který je využíván v infrastruktuře. Jako odesílatel byl nastaven email s názvem `alertsopenvas` s doménou infrastruktury.

6.2.4 Nastavení úkolů

Jakmile byly připraveny všechny předchozí kroky, bylo možné začít skenovat síť. Tím, že je vše připravené, je nastavování samostatných úkolů celkem jednoduché. Byly využity všechny předem připravené položky a jedinou zbylou věcí je vybrat skener a typ skenování. Pro všechny úkoly byl využit skener OpenVAS default a typ Full and Fast. Software nabízí dva přednastavené typy skeneru. Prvním je zmíněný OpenVAS default, který obsahuje základní funkce pro testovaní. Druhým skenerem je CVE, který umožňuje předvídat možná bezpečnostní rizika na základě aktuálních informací o zranitelnostech, které získá ze zprávy SecInfo. Na výběr je i z mnoha typů skenování [39]:

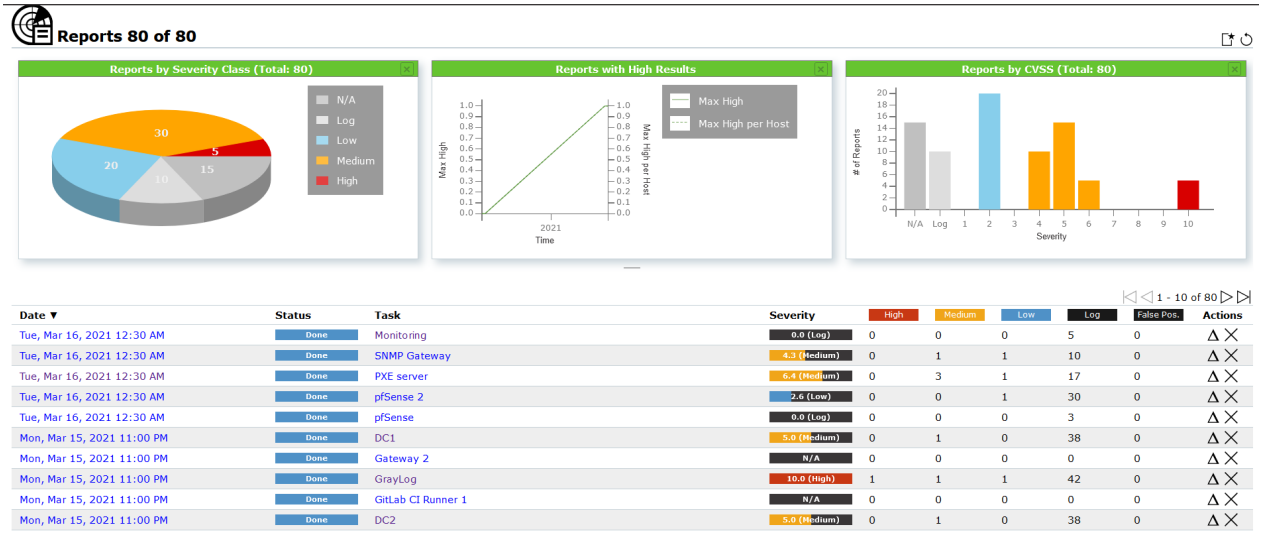
- **Discovery** - Konfigurace zjišťuje pouze informace o daném systému. Získané informace obsahují záznamy o otevřených portech, použitém hardwaru, použitých službách, bráně firewall a nainstalovaném softwaru.
- **Host Discovery** - Tato konfigurace se používá k detekci systémů.
- **System Discovery** - Konfigurace se používá k detekci cílových systémů včetně nainstalovaných operačních systémů a použitého hardwaru.
- **Full and Fast** - Konfigurace založena na informacích shromážděných v předchozím skenování portů a využívá téměř všechny NVT. Nepoužívá NVT, které by mohly způsobit kolaps na testovaném objektu. Jedná se o nejlepší volbu pro začátky skenování sítě.
- **Full and Fast Ultimate** - Konfigurace rozšiřuje předchozí metodu o NVT, které by mohly narušit služby, systémy nebo dokonce způsobit vypnutí.
- **Full and very deep** - Konfigurace skenování je podobná konfiguraci Full and Fast, ale výsledky skenování portů nebo detekce aplikace či služby nemají vliv na výběr NVT. Proto se používají NVT, která čekají na vypršení časového limitu nebo testují zranitelnost aplikace či služby, které nebyly dříve detekovány. Skenování s touto konfigurací je velmi pomalé.

- **Full and very deep ultimate** - Konfigurace rozšiřuje předchozí metodu o NVT, které by mohly narušit služby, systémy nebo dokonce způsobit vypnutí.

Průběh samotného skenu je pro cílový server velice výpočetně náročný a nelze na něm v danou chvíli pracovat. Test je opakován denně pro pravidelnou kontrolu. Aby se zamezilo zahlcení zprávami, bylo nastaveno automatické mazání zpráv, které jsou 5 dní staré. Není nutné uchovávat všechny, neboť vzniklé chyby budou zachyceny i v novějších zprávách. Tento krok je poslední v zajištění automatického skenování zranitelností na strojích. Následující kapitola se zabývá výsledky, které při těchto testech vznikají.

6.3 Výpisy proběhlého skenování

Cílem tohoto skenování je získání přehledu o tom, jak je daný stroj zabezpečený a případně objevit díry v zabezpečení. Výsledky testů se nachází ve webovém rozhraní v záložce *Scans/Reports*. Aniž bychom otevřeli jakoukoliv zprávu, získáme přehled už z grafického zobrazení, které můžete vidět na obrázku 6.3.

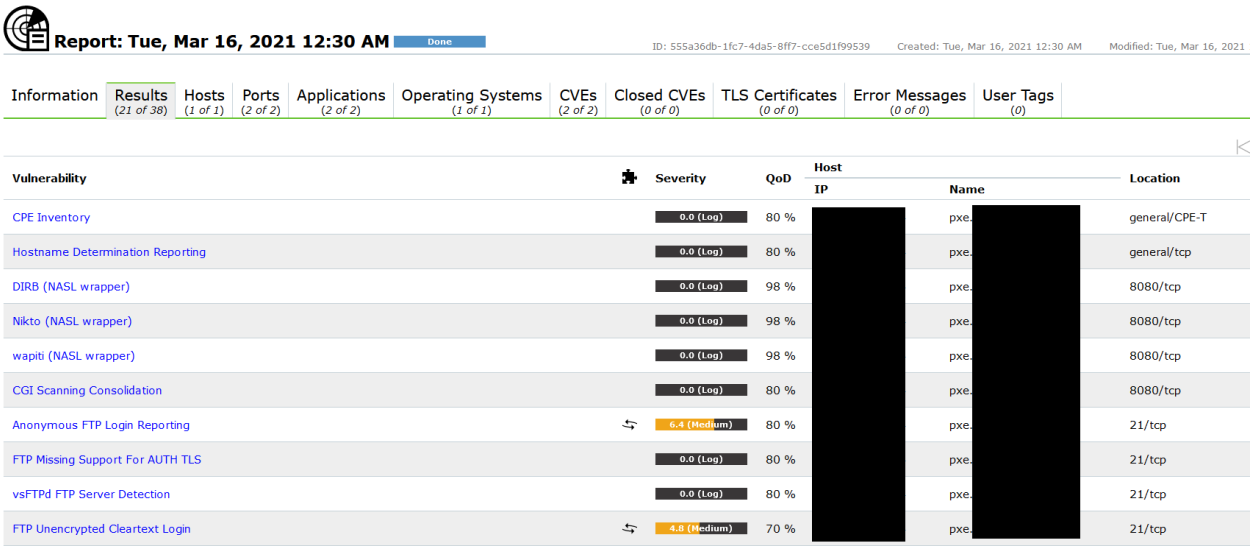


Obrázek 6.3: Dashboard záznamu o skenování

Pro detailnější informace je otevřen daný výpis. Pro ukázku bylo vybráno jedno hlášení, které zde bude popsáno pomocí obrázku 6.4.

Nejdůležitější záložkou je *Results*, ve které se nachází nalezené zranitelnosti. V listu zranitelností je vidět, které aktivity mají zvýšenou vážnost (severity). Každou zranitelnost lze rozbalit a o dané zranitelnosti získat přesnější informace. Lze se tak dozvědět přesný výsledek detekce, použité detekční metody a možné řešení tohoto problému. Další informace, které se nachází ve zprávě jsou:

- Hosti, kteří byli podrobeni tomuto typu testu. V tomto případě pouze jeden, neboť každý test je spouštěn na jednu IP adresu



Obrázek 6.4: Detalní zpráva o proběhlém skenování

- Porty, které byly využity během testování
- Operační systém a aplikace, které na hostu v danou chvíli běžely.

Každé hlášení je možné stáhnout do počítače v různých formátech např. PDF, Latex, XML a spousta dalších. Tato funkce může být využitá při prezentování těchto dat na poradách, nebo u vytváření vlastních statistik. Při dlouhodobém a pravidelném skenování je zajímavé pozorovat změny ve vážnosti proběhlých skenů. Dokáží odhalit neaktuální zařízení, vzniklé chyby během úprav konfigurace a mnoho dalšího.

6.4 Instalace IDS nástroje Suricata

Volba IDS nástroje by měla odpovídat požadovanému řešení. V konečné úvaze byly dva nástroje. Prvním z nich byla Suricata a druhým nástrojem byl Snort. Tyto dva nástroje jsou si velmi podobné a umí provádět téměř identické úkony. V infrastruktuře se využívá pfSense pro řízení síťového provozu. Běží v něm DHCP server, Firewall, NAT a další služby. Navíc právě pfSense nabízí spoustu balíčků, které mohou být přidány do jeho webového rozhraní. Jedním z nich je právě nástroj Suricata, ten díky pfSense získá grafické rozhraní v podobě HTML stránky. Lze tak přehledněji nastavovat pravidla pro sledování síťového provozu, sledovat výpisy logů a mnoho dalších věcí. Navíc je možné využít sadu pravidel od společnosti Snort, kterou Suricata podporuje.

Instalace samotného IDS nástroje je intuitivní a provádí se ve webovém rozhraní pfSense. Možnost přidávání balíčků se nachází v záložce *System*, kde je vybrán *PacketManager*. V něm jsou vidět všechny již nainstalované balíčky a v sekci *AvailablePackages*, je vyhledaná pod názvem Suricata.

Po dokončení instalace se objeví v nainstalovaných balíčcích a lze s ní začít pracovat. Suricata se nachází v pfSense v záložce *Services/Suricata*.

6.5 Konfigurace Suricaty

V tuto chvíli je instalace Suricaty dokončena a je možné začít s náročnější částí a to je konfigurace tohoto nástroje. Konfigurace je zaměřena na globální nastavení celého softwaru a na konfiguraci, která je specifická k vybranému rozhraní.

6.5.1 Globální konfigurace

Prvotním krokem po nainstalování softwaru je nastavení globální konfigurace nástroje. V globální konfiguraci je nutné nastavit základní vlastnosti, mezi které patří například nastavení, jaká pravidla se mají využívat, jak často se mají pravidla aktualizovat, nebo za jak dlouho má být zablokovaná adresa uvolněna.

Základem je nastavení pravidel, které pro sledování provozu chceme využívat. Suricata umožňuje využívat volně dostupná pravidla i jejich placená provedení. Placená pravidla mají značnou výhodu. Nově přidaná pravidla se v této verzi objeví ihned po jejich přidání do balíčku, oproti volně dostupným pravidlům, kde se tyto aktualizace objeví až za třicet dní. Suricata umožňuje využívat svá pravidla, ale také pravidla od nástroje Snort. To znamená větší variabilitu při nastavování specifických pravidel. Bylo povoleno využívání pravidel ETOpen, což jsou pravidla od společnosti Suricata a dále také využívání pravidel od společnosti Snort, jejich komunitní ruleset. Po zvolení pravidel bylo nutné přiřadit URL adresy, odkud se mají pravidla stahovat. Byla využita oficiální webová stránka od vývojářů pro zveřejňování pravidel `https://rules.emergingthreats.net/`, která nabízí URL odkaz pro ETOpen i Snort pravidla. Aktualizace pravidel jsou nastaveny jednou denně krátce po půlnoci. Tím je zajištěno automatické aktualizování balíčků pravidel, díky tomu nemusí být sledována správcem, zda nebyla přidána nějaká nová pravidla a bylo by nutné balíček aktualizovat ručně.

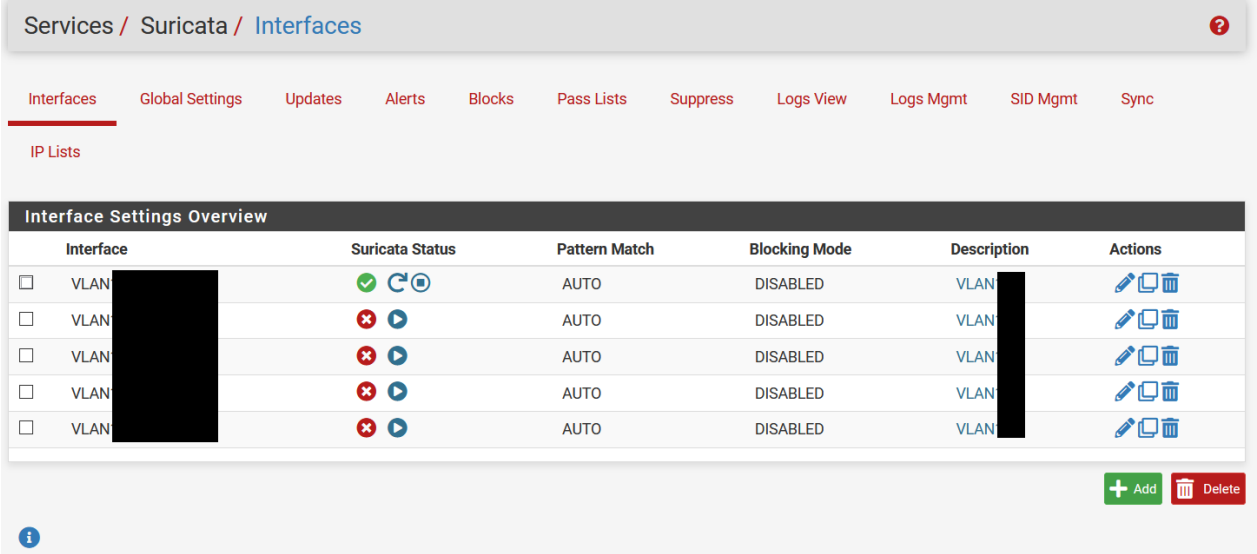
Poslední části globálních nastavení je určit dobu za jak dlouho má být blokovaná adresa uvolněna. Předem nastavená hodnota je jedna hodina. Hodnota byla snížena na dobu patnácti minut, kdyby došlo k mylné blokaci adresy. Dalšími možnostmi nastavení je nechat kopírovat zprávy od Suricaty přímo do systémového logu. Tato možnost nebyla využita a zprávy Suricaty jsou pouze v samotném logu.

6.5.2 Nastavení Suricaty pro sledování síťového provozu

Infrastruktura využívá několik rozhraní, převážně virtuálních LAN a jedno rozhraní WAN. Bylo nutné nastavit sledování síťového provozu pro každé rozhraní s výjimkou rozhraní WAN. Nastavení na tomto rozhraní je celkem zbytečné, zachycuje skenování portů i na portech, které jsou vypnuté

nebo nepoužívané. Generuje značnou část logů, které jsou pro správce Suricaty zcela irelevantní. Navíc využívá značnou část procesního výkonu, operační paměti a zahlcuje úložiště.

Podstatnější bylo vytvořit sledování síťového provozu pro zbylé interní rozhraní. Pro ukázku je popsáno nastavení pro rozhraní VLAN_A, které je v tuto chvíli nejvíce vytíženým rozhraním. Pro přidání nového rozhraní je nutné přejít do záložky Interfaces. Zde je možnost přidání nového rozhraní. Otevře se nová stránka viz obrázek číslo 6.5 , na které je řada záložek. Prvním krokem je zvolení rozhraní, na kterém se má spustit tato služba. Bylo tedy vybráno rozhraní VLAN_A a povolení Suricaty na tomto rozhraní.

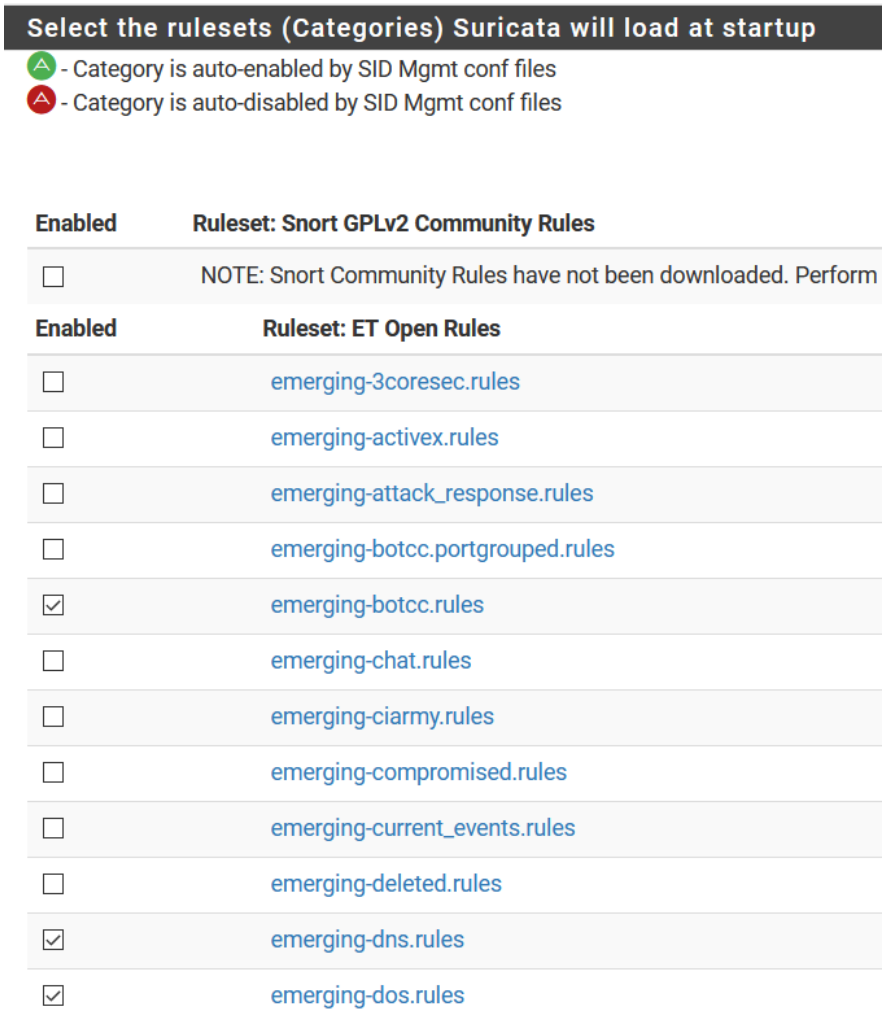


Obrázek 6.5: Vytvořená rozhraní pro detekci v Suricatě

Další krokem v nastavení je nastavení logů. Byl povolen zápis logů dekódovaného HTTP provozu na rozhraní. Je zapnuta funkce, která to do logu připisuje místo přepisování dat, která již byly zaznamenány. Dále je v této sekci možné povolit odesíláni upozornění do systémového logu, povolení TLS logů, ukládání souborů z toku aplikační vrstvy, logování dekódovaných paketů ve formátu pcap. Tyto funkce byly ponechány vypnuté, jelikož některé z nich jsou velmi hardwarově náročné. Poslední věcí, kterou lze v této části povolit, je zapnutí pořizování výkonových statistik. Tato funkce byla z počátku zapnuta, ale za pár dní došlo k zahlcení místa na disku a došlo k pádu celého softwaru pfSense. Z tohoto důvodu zůstalo toto nastavení vypnuté, jelikož obsah těchto logů je pro správce nedůležitý. Suricata dokáže získaná data zabalit a odeslat ve formátu JSON například na Syslog. Funkce je zatím nevyužita, ale v budoucnu se na tuto funkci bude zaměřovat a data se využijí k grafickému monitoringu, který v této infrastruktuře běží na softwaru Grafana. Bylo ponecháno vypnuté nastavení pro blokování hostů, kteří vytvoří nějaké upozornění. Prozatím bylo vynechané nastavení Suricaty jako IPS a využívá se tedy pouze část IDS, která slouží pro detekci. Zbylé nastavení v záložce *Settings* bylo ponecháno beze změny. Nemá vliv na detekci provozu, je zaměřeno

na výkon.

Následující dvě záložky *Categories* a *Rules* spolu úzce souvisí. V záložce `Categories` máme na výběr z řady kategorií pravidel, které je možné aktivovat. Mohou být aktivována všechna pravidla, ale tím dojde k velkému počtu upozornění, které nemusí znamenat žádné ohrožení. Začnou vznikat tzv. *False-positive*, které je třeba vyeliminovat následným laděním po spuštění Suricaty na daném rozhraní. Na obrázku číslo 6.6 je náhled kategorií, které jsou zvoleny pro VLAN_A.



Obrázek 6.6: Zvolené pravidla pro VLAN_A

Společnost Emerganing Threats vydala manuál, ve kterém jsou popsány funkce všech nabízených kategorií. V následujícím seznamu naleznete, jaké kategorie byly zvoleny a dozvíte se jejich základní funkci.

- **Botcc** zaznamenává automaticky vygenerované podpisy z různých zdrojů, které jsou potvrzené jako aktivní botnet.

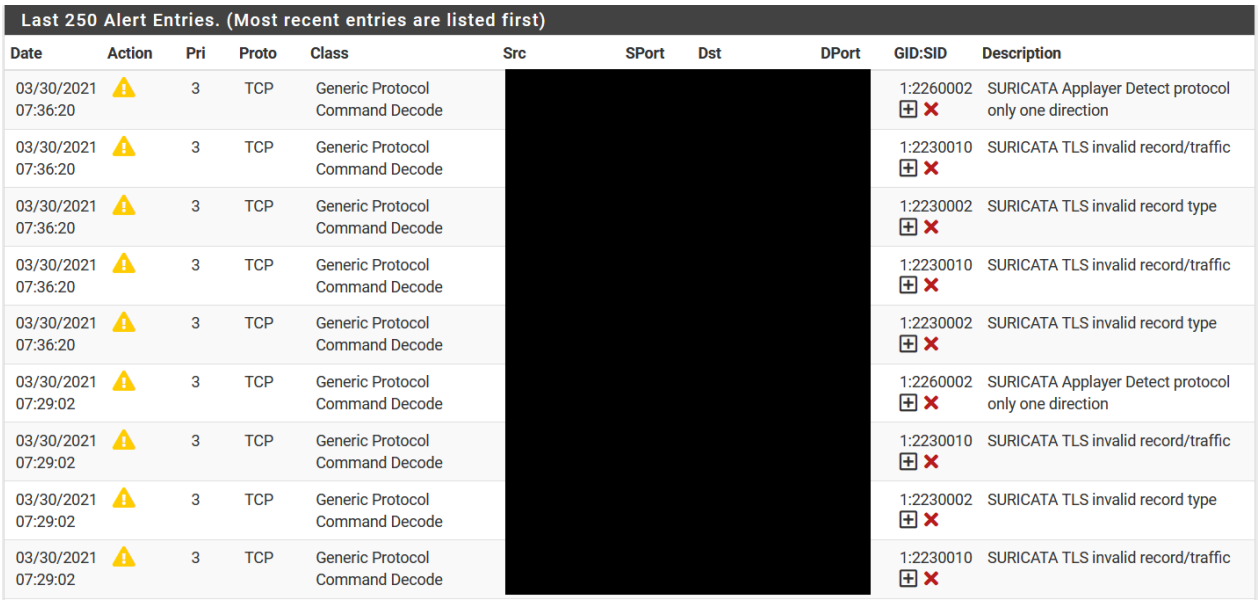
- **DNS** je určena pro podpisy s pravidly pro útok a chyby zabezpečení tykající se služby *DNS*.
- **DoS** je určena k zachycení příchozí aktivity *DoS* a poskytuje identifikaci odchozí aktivity *DoS*.
- **FTP** zajišťuje podpisy související s útoky, zranitelnostmi a zneužitím File Transport protokolu. Dokáže však monitorovat i nezávadnou aktivitu *FTP*.
- **IMAP** zajišťuje podpisy související s útoky, zranitelnostmi a zneužitím služby *IMAP*. Dokáže však monitorovat i nezávadnou aktivitu pro účely protokolování.
- **Malware** detekuje podpisy škodlivých softwarů. Pravidla této kategorie zjišťují aktivitu související se škodlivým softwarem, který byl v síti detekován. Dokáže rozpoznat přenášené malwary, aktivní malwary, malwarové útoky či jejich aktualizace. Jedná se o jednu z nejdůležitějších kategorií, které právě ETOpen nabízí.
- **Web Server** je určena k detekci útoků na infrastrukturu webových serverů jako jsou Apache, Nginx, Microsoft IIS a další. [40]

Tímto je dokončeno konkrétní nastavení pro VLAN_A. Jelikož v infrastruktuře není žádná speciální VLAN, která by vyžadovala přidání nějakých specifických pravidel, bylo využito klonování vytvořené VLAN_A. Na zbylých VLAN je prozatím minimální provoz, proto dále bude demonstrace probíhat na VLAN_A. Nyní je možné na tomto rozhraní spustit službu Suricata, která začne sledovat síťové dění. Po spuštění se začne objevovat řada upozornění, která jsou nutná odladit. Tato problematika bude popsána v následující podkapitole.

6.6 Výpis upozornění

Hlavním důvodem použití Suricaty je monitoring síťového provozu. I při použití menšího počtu pravidel dochází k vytváření tzv. *false-possitive* upozornění, proto je důležité postupem času tato upozornění odstranit. V nynějším stádiu nastavení, je Suricata nastavena pouze jako detekční systém, proto je nutné pravidelně kontrolovat jisté nesrovnalosti v těchto výpisech. Na obrázku číslo 6.7 můžete vidět ukázku výpisu uložených záznamů.

Záznamy jsou prezentovány pod sebou a v tomto zobrazení je jich pouze posledních 250. Pro nahlédnutí do starších upozornění je potřeba nahlédnout do logu `alerts.log`, který je uložen na serveru. O záznamu se ukládají potřebné informace pro zjištění daného problému. Nejdůležitějším sloupcem je *GID:SID*. *GID:SID* umožňuje identifikovat daný problém podle napsaného pravidla. Jednoduchým řešením je využití internetového vyhledávače pro rychlou identifikaci problému. Na internetu je k nalezení spousta užitečných fór, kde se na tento problém někdo dotazoval a zkušenější správci dávali rady, zda se jedná o *false-possitive* či je toto upozornění užitečné. Dále se z těchto informací dozvíme o samotné komunikaci. Je uvedena IP adresa a port zdrojového počítače, tak i



Last 250 Alert Entries. (Most recent entries are listed first)

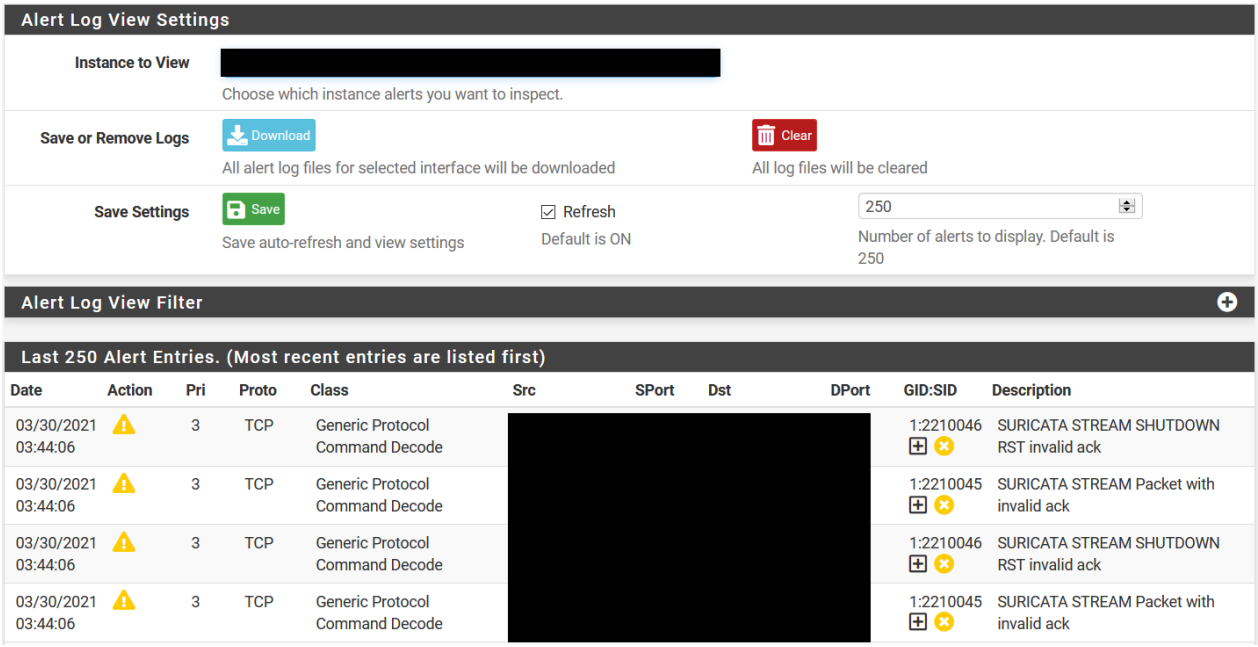
Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
03/30/2021 07:36:20	⚠	3	TCP	Generic Protocol Command Decode	[redacted]				1:2260002	SURICATA Applayer Detect protocol only one direction
03/30/2021 07:36:20	⚠	3	TCP	Generic Protocol Command Decode					1:2230010	SURICATA TLS invalid record/traffic
03/30/2021 07:36:20	⚠	3	TCP	Generic Protocol Command Decode					1:2230002	SURICATA TLS invalid record type
03/30/2021 07:36:20	⚠	3	TCP	Generic Protocol Command Decode					1:2230010	SURICATA TLS invalid record/traffic
03/30/2021 07:36:20	⚠	3	TCP	Generic Protocol Command Decode					1:2230002	SURICATA TLS invalid record type
03/30/2021 07:29:02	⚠	3	TCP	Generic Protocol Command Decode					1:2260002	SURICATA Applayer Detect protocol only one direction
03/30/2021 07:29:02	⚠	3	TCP	Generic Protocol Command Decode					1:2230010	SURICATA TLS invalid record/traffic
03/30/2021 07:29:02	⚠	3	TCP	Generic Protocol Command Decode					1:2230002	SURICATA TLS invalid record type
03/30/2021 07:29:02	⚠	3	TCP	Generic Protocol Command Decode					1:2230010	SURICATA TLS invalid record/traffic

Obrázek 6.7: Ukázka výpisu pro VLAN_A

IP adresa a port cílového počítače. Sloupec Class je také užitečný pro rychlou identifikaci daného problému.

Všechny zjištěné *false-possitive* je nutné eliminovat. Výhodou Suricaty je umožnění vypnutí pravidel v reálném čase během provozu. Slouží k tomu malý křížek, který se nachází u `GID:SID`. Pravidlo je okamžitě vypnuto a další upozornění se již nebude zobrazovat. Výhodou je uživatelsky přívětivé ladění této služby, neboť není nutné po každém nalezeném *false-possitive* restartovat celou službu. Na obrázku 6.8 můžete vidět příklad tzv. *false-possitive*, který byl již vypnut.

Ladění tohoto softwaru je tzv. mravenčí prací, jelikož je použito mnoho pravidel, které je nutné postupně odladit. Při kontrole záznamů byl viděn průběh kontroly, který byl prováděn softwarem OpenVAS. Ze záznamů bylo patrné, že proběhl pokus o prolomení hesel, přidělení administrátorských práv a podobně. Tyto záznamy patřili k těm užitečnějším, neboť většina upozornění není úplně zajímavá, protože je tvořena *false-possitive* upozorněními.



Obrázek 6.8: Ukázka výpisu pro VLAN_A

Kapitola 7

System Center Manager

Tato kapitola se zaměří na software System Center Configuration Manager. Jedná se o software, který umožňuje jednodušeji spravovat všechny počítače v doméně s operačním systémem od společnosti Microsoft. V kapitole bude popsána instalace softwaru a konfigurace vybraných funkcí, které se řadí k těm nejpoužívanějším. Během instalace bylo vycházeno z knihy System Center 2012 R2 Confugariton Manager, na kterou bude odkazováno. [36]

7.1 Instalace SCCM

Instalace System Center Configuration Manager je velmi rozsáhlá a je nutné spoustu věcí připravit před samotnou instalací. V následujících kapitolách bude popsáno, jak se při instalaci postupovalo.

7.1.1 Příprava před instalací

Pro zprovoznění výkonného konfiguračního manažera, je nutné správně rozložit úložiště, přiřadit dostatek operační paměti a procesorů pro SQL Server. Pro instalaci jsou potřeba minimálně dva Windows servery. Na prvním Windows serveru musí být nainstalovány následující role:

- DNS
- DHCP
- Active Directory Domain Controller

Server je uložen pod doménovým jménem DC1. Druhý Windows Server musí splňovat odlišné role, které jsou využívány konfiguračním manažerem. Server je v doméně uložen pod názvem CM01 a zde jsou uvedeny role, které bude zastupovat:

- Management Point
- Software Update Point

- Distribution Point
- Application Catalog Web Service Point
- Application Catalog Website Point

Na serveru DC1 je možné přidat rozšiřující schéma pro Active Directory. Instalace je vykonána přes příkazový řádek. Pomocí příkazové řádky je otevřena složka `SMSSETUP/BIN/x64`, ve které se nachází instalační soubory pro konfiguračního manažera. Instalace tohoto rozšíření se spouští pomocí `exttadsch.exe` souboru. Po dokončení je nutné ověřit, zda byla schémata úspěšně přidána. K tomu slouží `ExtADSch.log`, který se nachází na disku C:. Tato část je nutná pro vytvoření kontejneru, který se používá k uložení zveřejněných dat, jako jsou například certifikáty. Site server dokáže tento kontejner vytvořit během instalace, ale je nutné přiřadit kontejneru plné administrátorské práva. Z tohoto důvodu je lepší provést instalaci manuálně pomocí `adsiedit.msc`. V Active Directory se vytvoří nová skupina s názvem *ConfigMgr_Servers* v organizační jednotce *Contoso/Security Groups*. Do ní byl přiřazen nově vytvořený primární Site Server CM01. Následujícím krokem bylo vytvoření samotného kontejneru, který se vytváří v *ADSI Edit*. Posledním krokem je skupině ConfigMgr přiřadit plná administrátorská práva.

ConfigMgr a SQL server mohou pracovat v kontextu účtu místního systému. Pro SQL server je tento postup považován za nejlepší z pohledu zabezpečení. Vytváří účty s omezeným oprávněním a používá jej jako servisní účet. Pro ConfigMgr počet potřebných účtů závisí na funkcích, které mají být konfigurovány. Pro lepší správu těchto účtů, je nutné provést konfiguraci Group Policy objects zkráceně GPo. GPo se využívá:

- pro konfiguraci Windows firewallu
- pro konfiguraci lokálního Windows Server Update Service
- pro přidání klientského účtu do lokální administrátorské skupiny

Jak již bylo zmíněno, je nutné upravit práva v bráně firewall. Musela se udělit výjimka pro příchozí vzdálenou správu, a také výjimka pro příchozí sdílení souborů a tiskáren. Ve WSUS bylo povoleno stahování aktualizací z intranetu Microsoftu a byla zakázána automatická konfigurace těchto aktualizací.

7.1.2 Instalace SQL serveru

V minulé podkapitole bylo zmíněno, že součásti instalace SCCM je instalace a konfigurace vlastního SQL serveru. Z pohledu hardwaru SQL Server podporuje běh až na třiceti dvou jádrech a 64GB operační paměti. Minimální velikost operační paměti je 8GB pro SQL server a 8GB pro primární server. Byla provedena instalace lokálního SQL serveru, neboť nabízí jednodušší správu oprávnění

Disk	Použití	Velikost disku
C:\	Operation System	100 GB
D:\	ProgSYS	100 GB
E:\	Content Library	200 GB
F:\	TempDB	50 GB
G:\	SQLDB	200 GB
H:\	SQLLOG	200 GB

Tabulka 7.1: Rozložení disku pro CM01 [36]

a počet klientů infrastruktury z daleka nedosahuje maxima lokálního SQL serveru. V softwaru VMware vSphere bylo nutné přidat pět virtuálních disků k serveru CM01 viz tabulka 7.1. [36]

Na serveru DC1, který zastupuje roli Active Directory, byla vytvořena nová skupina s názvem *ConfigMGR_Admins*, aby administrátoři získaly přístup k SQL databázi. Poté byla provedena instalace samotného SQL serveru na serveru CM01. Po dokončení instalace byla provedena kontrola v SQL manažeru, zda byla přiřazena *Master* databáze. Dalším krokem pro úspěšné nastavení SQL serveru je konfigurace paměti. Jak bylo již v předchozím textu zmíněno, SQL serveru bylo přiřazeno 8GB operační paměti.

V základním nastavení SQL Server využívá port 1443 pro klasickou SQL komunikaci a port 4022 pro komunikace se Server Broker [36]. Během instalace SQL serveru se zobrazí upozornění, že tyto porty nebyly správně nakonfigurovány v bráně firewall. Bylo přidáno pravidlo pro protokol TCP, aby porty 1433 a 4022 byly zpřístupněny a bylo umožněno připojení přes tyto porty.

Posledním krokem pro dokončení instalace SQL serveru je vytvoření databáze pro konfigurační manažer. Databáze se skládá z dvou souborů:

- **Databázové soubory** ukládají objekty, tabulky, indexy a uložené procedury
- **Transakční protokol** ukládá veškeré databázové transakce

Bylo využito manuální vytvoření databáze, z důvodu větší kontroly nad počtem databázových souborů a konfigurací každé části na přesně stejnou velikost.

7.1.3 Instalace Site serveru

Před samotnou instalací je nutné na serveru CM01 nainstalovat a nastavit službu WSUS. Instalace WSUS byla provedena pomocí skriptu v PowerShellu. WSUS byl nastaven, aby ukládal všechny stažené aktualizace lokálně na disk E:. Pro tento krok byl využit skript, který je uveden v knize. [36]

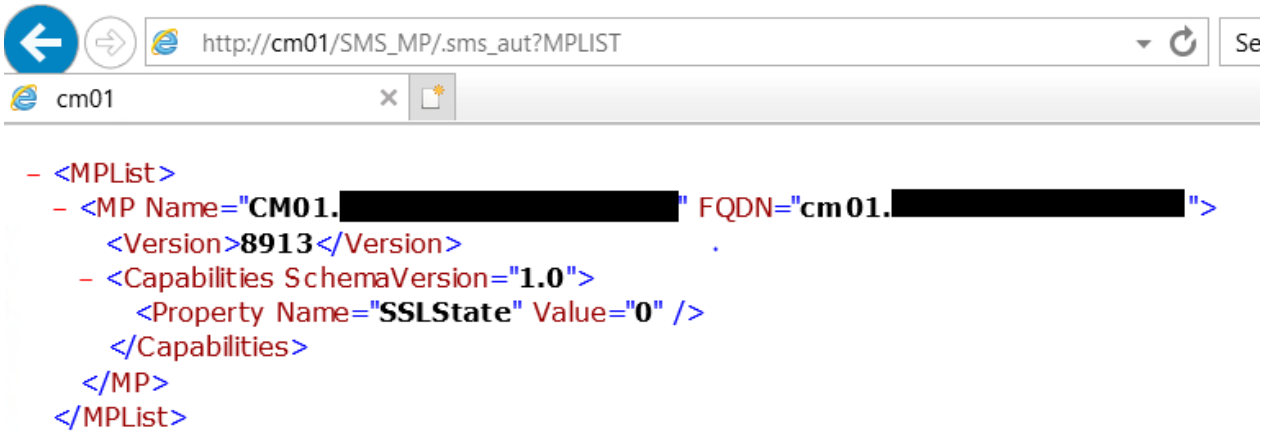
Před samotnou instalací primárního Site serveru je nutné vědět, jak má vypadat finální hierarchie. Po instalaci již není možné provádět změny v hierarchii. Nainstalování Site serveru požaduje

mít nainstalovaný Windows Assesment and Deployment Kit. Během instalace této služby byly zvoleny pouze tři komponenty:

- Deployment Tools
- Windows Preinstallation Enviroment
- User State Migration Tool

Nyní je vše připraveno k dokončení instalace konfiguračního manažera. Pro pokračování stačí spustit instalační soubor pomocí příkazového řádku. Během instalace byly potvrzeny všechny nezbytné podmínky a licenční smlouvy. V části *Site and Installation Settings*, bylo nutné vyplnit *Site code*, *Site name* a instalační adresář. Poté se postupovalo pokyny, které byly kladeny během instalace.

Po dokončení instalace byla provedena kontrola, zda vše úspěšně proběhlo. Pro kontrolu bylo nahlédnuto do dvou logů, které jsou uloženy v adresáři konfiguračního manažera. K procházení logů byl použit program CMTrace pro přehlednější výpis. Log `sitecomp.log` slouží pro Site Component Manager, který odpovídá za instalaci většiny komponentů pro konfiguračního manažera. Druhým užitečným logem je `hman.log`. Tento log zaznamenává běh *Hierarchy Manager*, který zodpovídá za aktualizování Active Directory, zpracovávání certifikátů a dalších. Pro ověření lze zkontrolovat také management point pomocí internetového prohlížeče. Na obrázku číslo 7.1, lze vidět příkaz pro výpis MP a samotný výpis všech MP. [36]



Obrázek 7.1: Ověření Management Point

Tímto byla úspěšně dokončena instalace System Center Configuration Manager 2016. V následující kapitole bude popsána základní konfigurace softwaru.

7.2 Konfigurace SCCM

V předchozí kapitole byla popsána instalace konfiguračního manažera. Toho je po instalaci nutné správně nastavit, aby mohly být využívány všechny služby, kterými disponuje. Již na začátku bylo zmíněno, že všechny role běží pouze na primárním Site Serveru, neboť počet uživatelů a strojů v infrastruktuře nezahltí konfigurační manažer. Toto řešení však není jediné. U větších infrastruktur by bylo vytvořeno více sekundárních Site serverů za účelem rozdělení rolí, aby se zamezilo ztrátě výkonu konfiguračního manažera.

7.2.1 Instalace rolí

Přiřazení rolí se nachází v konfiguračním manažeru v sekci *Administration/Servers and Site System Roles*, kde je zobrazen primární server. Na primární Site server byly přiřazeny následující role:

- Software Update Point
- Asset Intelligance Synchronization Point
- Reporting Service Point

Po dokončení výběru byly služby, zvolené v předchozím kroku, postupně nastaveny. V nastavení Software Update Pointu, bylo důležité změnit nastavení pro WSUS, který standardně komunikuje na portech 8530 a 8531 a bylo povoleno připojení s klienty pouze přes intranet. Byl také povolen plánovač synchronizací. Ten je nastaven tak, aby byl synchronizován každých 8 hodin. Kdyby v průběhu synchronizace došlo k chybě, tak v konfiguračním manažeru se zobrazí upozornění. Tyto upozornění se nachází v sekci *Monitoring*. Synchronizovat se budou pouze aktualizace s označením *Critical updates, Definition updates, Security updates a Service packs*. Zda synchronizace funguje lze ověřit v `wsyncmgr.log`, který zaznamenává průběh WSUS synchronizace. Pro nastavení *Asset Intelligance sychronization point* bylo využito defaultní nastavení. Posledním krokem byla konfigurace služby Reporting Service Pointu. V nastavení byl přiřazen SQL server a provedlo se ověření propojení s databází.

Konfigurační manažer má mnoho komponentů, které jsou zapojeny do procesu konfigurace a instalace systémových rolí. Proto je důležité při konfiguraci kontrolovat příslušné logy, které souvisí z danou službou. Užitečné logy pro kontrolování aktivit SQL Reporting Services a správného běhu WSUS jsou:

- `srsrpMSI.log`
- `srsrp.log`
- `srsrpsetup.log`
- `WCM.log`

- `WSUSCtrl.log`
- `wsyncmgr.log`

Každá aktivita, která běží v konfiguračním manažeru, má příslušný log soubor, který zaznamenává průběh určité aktivity. Pomocí internetu nebo knihy je jednoduché nalézt název příslušného logu a zkontrolovat, kde nastala případná chyba. [36]

7.2.2 Konfigurace úkolů údržby

Dalším krokem bylo nastavení zálohování a dalších úkolů údržby. Konfigurační manažer poskytuje grafické rozhraní pro správu vlastností údržby a správu SQL databázového serveru. Nemuselo být využito nativní rozhraní pro SQL server, aby se mohla spravovat databáze. Bylo nutné provést nastavení denní zálohy konfiguračního manažera, týdenní aktualizaci indexů na SQL serveru a vyčištění neaktivních a zastaralých klientů. Konfigurace se provádí v sekci *Administration/Sites* a na primárním serveru byla zvolena možnost *Site Maintenance*. Na obrázku 7.2 je vidět část úkolů, které jsou nastaveny na dané dny a čas, kdy mají na serveru probíhat.

Icon	Name	Enabled	Schedule Start After	Schedule Latest Start Time	Days of the Week
	Delete Aged Replication Summary Data	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat
	Delete Aged Status Messages	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat
	Delete Aged Threat Data	Yes	12:00 AM	5:00 AM	Sat
	Delete Aged Unknown Computers	Yes	12:00 AM	5:00 AM	Sat
	Delete Aged User Device Affinity Data	Yes	12:00 AM	5:00 AM	Sat
	Delete Expired MDM Bulk Enroll Packa...	Yes	12:00 AM	5:00 AM	Sat
	Delete Inactive Client Discovery Data	Yes	12:00 AM	5:00 AM	Sat
	Delete Obsolete Alerts	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat
	Delete Obsolete Client Discovery Data	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat
	Delete Obsolete Forest Discovery Sites...	Yes	12:00 AM	5:00 AM	Sat
	Delete Orphaned Client Deployment S...	Yes	12:00 AM	5:00 AM	Sat
	Monitor Keys	Yes	12:00 AM	5:00 AM	Sun
	Rebuild Indexes	Yes	12:00 AM	4:00 AM	Sun
	Summarize File Usage Metering Data	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat
	Summarize Installed Software Data	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat
	Summarize Monthly Usage Metering...	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat
	Update Application Available Targeting	Yes	12:00 AM	5:00 AM	Sun, Mon, Tue, Wed, Thu, Fri, Sat
	Update Application Catalog Tables	Yes	12:00 AM	11:59 PM	Sun, Mon, Tue, Wed, Thu, Fri, Sat

Obrázek 7.2: Ukázka úloh údržby pro primární server

Konfigurace zálohy je řešena na SQL serveru, místo využití zabudované úlohy pro údržbu. Bylo nutno zálohovat Reporting Server, WSUS a databázi. Ani jedna z těchto služeb není zahrnuta v zabudované úloze údržby v konfiguračním manažeru. To bylo hlavním důvodem využití zálohy na SQL serveru oproti zabudované úloze. Záloha na SQL serveru podporuje kompresi dat a nepřeruší žádné služby, která je využívána v konfiguračním manažeru. Nastavení se nachází v konfiguračním manažeru v záložce *Tools/Services* ve vlastnostech služby SQL Server Agent. Služba je nastavena

na automatické spuštění s krátkým zpožděním po zapnutí serveru. V SQL Server Management studiu po připojení k primárnímu Site serveru CM01 se spustil Maintenance Plan Wizard. Zde bylo provedeno nutné nastavení, aby se choval jako připravený SQL Server Agent. V plánovači bylo provedeno nastavení pravidelného spouštění. Probíhá v denním cyklu, který se spustí v jednu hodinu ráno. Mezi úkoly, které bude vykonávat, byly vybrány:

- **Zálohování databáze** - Týká se to databáze: *CM_PS1*, *ReportServer* a *SUSDB*. Bylo přiřazeno místo, kde se má záloha ukládat. Využilo se připraveného disku G:, který je určen pro zálohu databáze. Pro ušetření místa na disku jsou data komprimována.

- **Mazaní staré zálohy** - Všechny zálohy, které jsou starší než týden, jsou pravidelně mazány, aby nedocházelo k zahlcení disku.

7.2.3 Konfigurace Discovery

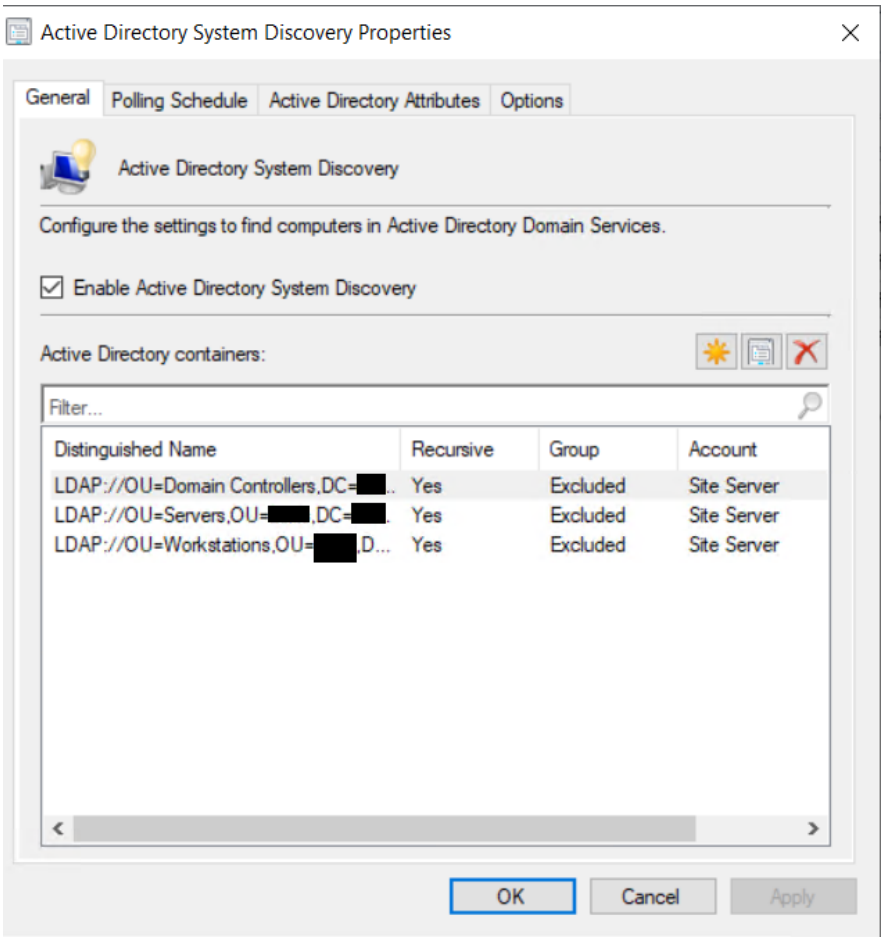
Discovery je proces, při kterém se konfigurační manažer dotazuje předdefinovaného zdroje a hledá základní informace o daném objektu. Jsou různé metody, kterými se lze dotazovat a každá z nich se používá pro jiné účely. V následující tabulce číslo 7.2 je vidět, které metody jsou zvoleny a jaká je jejich funkce. [36]

Metoda objevování	**Funkce metody**	**Proč se využívá**
Active Directory Forest	Zjišťuje sítě a IP rozsahy v Active Directory.	Používá se k automatickému vytváření hranic, minimalizuje manuální práci.
Active Directory System	Zjišťuje objekty počítačů a získává informace, jako jsou základní informace o stroji, informaci o organizační jednotce a další	Je dobré vidět všechny objekty počítačů před instalací klientů. Díky této metodě můžeme vytvořit kolekce založené na operačním systému a lokaci.
Active Directory User	Zjišťuje informace o uživatelích.	Nutné pro správnou distribuci aplikací, rozdělení do specifických kategorií.
Active Directory Group	Zjišťuje security group v Active Direcoty	Nutné pro správnou distribuci aplikací, rozdělení do specifických kategorií.

Tabulka 7.2: Použité metody objevování

Poslední metoda, která už není zahrnuta do tabulky, je metoda *Heartbeat*. Tato metoda získává data, které slouží pro nastavení správy inventáře a reportingu. Metoda je také známa pod názvem Discovery Data Collection Cycle, který zaznamenává data jako název počítače, doménové jméno, název operačního systému či posledního přihlášeného uživatele. Výchozí stav této metody je aktivní. Pozměněn byl pouze interval obnovy ze sedmi dnů na jeden den. Tento provoz je sice paměťově náročnější, generuje asi 10KB dat za jednoho klienta, ale při aktuálním počtu klientů v infrastruktuře nedojde k zahlcení přiřazeného disku. Výhodou je výrazně aktuálnější konzole konfiguračního manažera.

Konfigurace se opět provádí v konfiguračním manažeru v sekci *Administration/Overview/Hierarchy Configuration/Discovery Methods*. Jako první se provedlo nastavení Active Directory Forest Discovery. V této službě se povolilo automatické vytváření hranic (boundaries) a automatické vytvoření IP rozsahu z nově zjištěných informací. Funkce se spouští jedenkrát týdně. Dalším krokem bylo nastavení Active Director System Discovery. Byla vytvořena nová pravidla pro přidání všech LDAP cest viz obrázek číslo 7.3. V *Options* je nakonfigurován interval, který limituje vyhledávání nových serverů či desktopů v doméně. Vyhledávají se pouze stroje, které se v posledních 30 dnech přihlásily do domény a jejich heslo bylo aktualizováno v posledních 90 dnech.



Obrázek 7.3: Active Directory System Discovery

Metoda Active Directory User potřebovala doplnit cestu k uživatelům uloženou v Active Directory. V nastavení vyhledávání bylo nastaveno rekurzivní vyhledávání. Podobně byla nastavována také metoda Active Directory Group, kde místo cesty k uživatelům byla uvedena cesta k Software Groups. V nastavení bylo opět přidáno omezení pro vyhledávání strojů.

Po dokončení konfigurace je vždy nutné ověřit funkčnost. Jelikož Discovery procesy běží na pozadí, měly by generovat záznamy dat v konzoli konfiguračního manažera. Aby byla ověřena funkčnost

Prefix kolekce	Vytvořená ve složce	Účel kolekce
CO	Contoso	Slouží k zabezpečení na základě rolí. Obsahuje Domain Controlery, všechny Windows servery a desktopy.
EP	Endpoint Protection	Používá se pro ovládání funkcí EP
SWD (pro device collection) SWU (pro user collection)	Software	Slouží k řízení nasazování aplikací.
CM	Compliance Management	Slouží k řízení souladu. V Contoso jsou dvě složky tohoto typu. Jedna slouží pro uživatele a druhá pro zařízení
OSD	Operating System Deployment	Slouží k řízení nasazování operačních systémů. Během obsluhy instalace jsme schopni číst data a proměnné z kolekce.
SUM	Software Updates	Slouží k řízení softwarových aktualizací.

Tabulka 7.3: Rozložení a účel dané kolekce

AD Forest Discovery, je nahlédnuto v konzoli do záložky *Administration* a v *Overview/Hierarchy Configuration/Bounderies* lze vidět, zda byla vytvořena nějaká hranice. Dále bylo zkontrolováno úspěšné vytvoření Active Directory Forests a byl ověřen *discovery a publishing* status. Z *publishing statusu* lze říct, že cokoliv konfigurační manažer provede, dokáže data úspěšně zapsat do Active Directory. Ověření zda z Active Directory dostává konfigurační manažer informace o serverech, které jsou zde uloženy, se nachází v záložce *Assets and Compliance/Overview/Devices*. Na každý sesrver lze kliknout a rozbalit si získané informace. Stejným způsobem jsou ověřováni i uživatelé, kteří jsou vytvořeni v doméně infrastruktury.

7.2.4 Kolekce

Vytvoření kolekcí je posledním krokem k dokončení konfigurace. Kolekce se skládá z jednoho či více objektů, které jsou logicky seskupeny, aby sloužili pro specifické účely. Základní chybou je využívání funkcí bez vytvoření příslušných kolekcí. Kolekce mohou být zaměřeny:

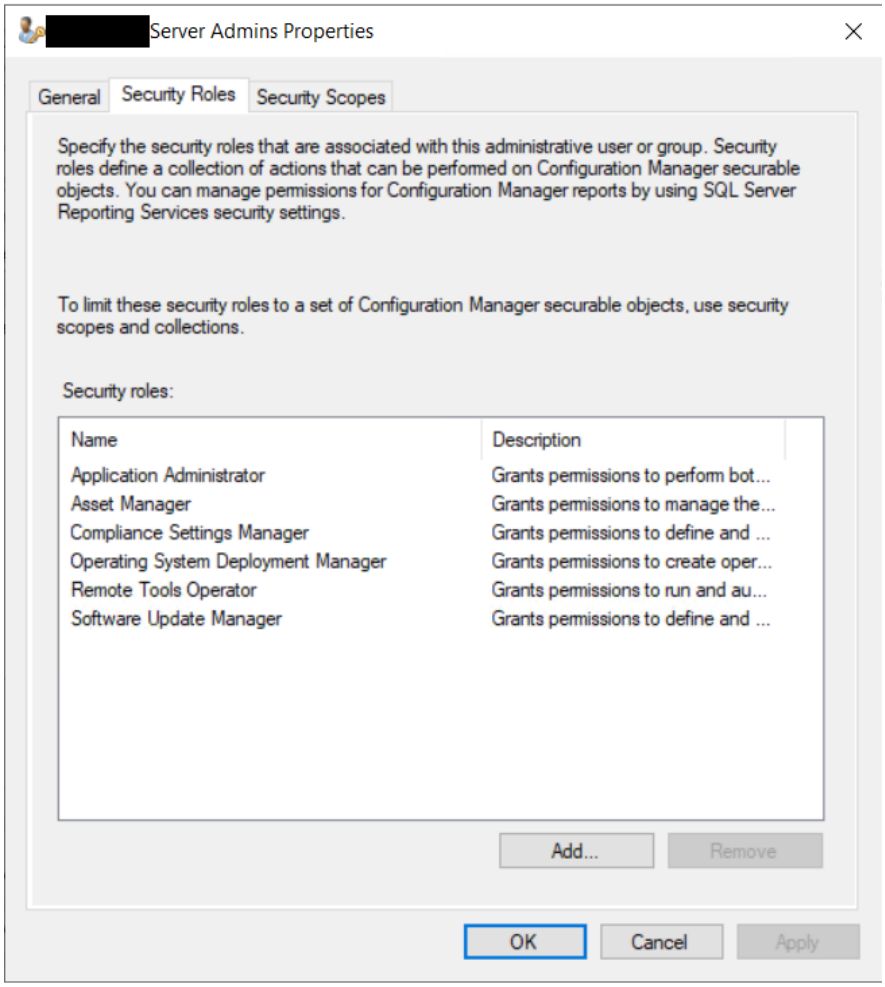
1. Na kontrolu bezpečnosti
2. Podporou pro řízení využívaných funkcí
3. K minimalizaci potřebného SQL kódu v hlášeních

Při rozdělování do určitých kolekcí, byl využit návrh rozvržení kolekcí, který je uveden v knize a finální rozdělení kolekcí si můžete prohlédnout v tabulce 7.3. [36]

Složky byly tvořeny manuálně, ale lze využít i jednoduchého PowerShell skriptu, který byl pro vytvoření pár složek nepotřebný. Po vytvoření složek byly vytvářeny příslušné kolekce k zajištění

zabezpečovacího modelu. Jako první byla vytvořena kolekce s názvem *CO All Servers*, která pokrývá veškeré Windows servery, které jsou přidány do domény. Limitování této kolekce je nastaveno na všechny servery. Bylo nutné vytvořit pravidlo pro získávání informací z databáze, které vyhledává atribut s názvem a verzí operačního systému u každého serveru. Pro tuto kolekci bylo povoleno automatické aktualizování kolekce. Další kolekce byla nastavena téměř totožně, ale při výběru byly vybrány pracovní stanice. Kolekce je uvedena pod názvem *CO All Workstations*. Tímto způsobem byly vytvořeny potřebné kolekce, pomocí kterých lze omezovat přiřazování aplikací, nasazování nových aktualizací a spoustu dalších funkcí.

Pro správu bylo nutné v Active Directory vytvořit dvě skupiny Server Admins a Workstation Admins. Byly vytvořeny dva nové účty, které byly přiřazeny do příslušné skupiny: Server Admins a Workstation Admins. Následně v konfiguračním manažeru v záložce *Administration/Administrative/User* byly vytvořeným skupinám přiděleny příslušné bezpečnostní role, které jsou zobrazeny na obrázku 7.4.



Obrázek 7.4: Vybrané bezpečnostní role pro Server Admins

Pro pracovní stanice byly využity stejné role a ještě k nim byla přidána role *Company Resource Access Manager*, která uživatelům a zařízením uděluje oprávnění k vytváření, správě a nasazování profilů přístupu k prostředkům společnosti, jako jsou Wi-Fi, VPN a profily certifikátů.

Na závěr této podkapitoly, je uvedeno pár užitečných logů, které dokáží sledovat údržbu, Discovery proces a aktualizace kolekcí. `Adsysdis.log` zaznamenává aktivity spojené s Active Directory System Discovery procesem. Zaznamenává také základní informace o serverech. Běžnou chybou v tomto procesu bývají chybějící oprávnění. Podobný log je i pro uživatelský proces zjišťování a nachází se názvem `adusrdis.log`. Pro kontrolu hledání nových bezpečnostních skupin, je využíván log `adsgdis.log`. Konfigurační manažer nabízí spoustu užitečných logů, které mohou vést k vyřešení problému a díky CMTraceLog manažera, jsou logy velmi přehledné.

7.3 Nastavení automatických aktualizací pro Windows

Udržovat Windows a softwary třetích stran aktuální je pro bezpečnost velmi důležité. Při plánování softwarových aktualizací je nutné dodržovat tyto základní kroky:

- Musí být snadné schvalovat a nasazovat nové aktualizace
- Žádné aktualizace nesmí být nainstalovány bez důkladného otestování
- Všechny servery musí být součástí aktualizačního plánu
- Musí existovat plán pro nejméně přijatelnou úroveň souladu

Řešení softwarových aktualizací se skládá z dvou částí a to z aktivního softwarového bodu s nainstalovaným WSUS a z klienta konfiguračního manažera. WSUS a aktivní softwarový bod byl nakonfigurován na serveru CM01, který zároveň slouží jako konfigurační manažer. Také je nutné připojení serveru k internetu, aby mohly být stahovány nové aktualizace.

Software Update Point se skládá ze tří komponentů. Prvním komponentem je WSUS Control Manager. Ten zodpovídá za funkčnost WSUS serveru. Každou hodinu kontroluje jeho stav a aktivitu zapisuje do souboru `WSUSctrl.log`, který je umístěn na WSUS serveru. Dalším komponentem je WSUS Configuration Manager, který slouží ke konfiguraci WSUS nastavení. Změnit nastavení lze kdykoliv ve vlastnostech Software Update point. Nastavení se nachází v sekci *Administration/Sites* v konfiguračním manažeru. Poslední komponenta je WSUS Synchronization Manager, která zařizuje synchronizační proces mezi Microsoft Windows Update a WSUS serverem, a také mezi WSUS serverem a konfiguračním manažerem.

7.3.1 Software Update kolekce

Jako u všech ostatních služeb i tato má vlastní kolekci vytvořenou na míru. Usnadňuje testování a nasazování nových verzí operačních systému, či jiných systémových aktualizací. Proto bylo zvoleno toto rozvržení.

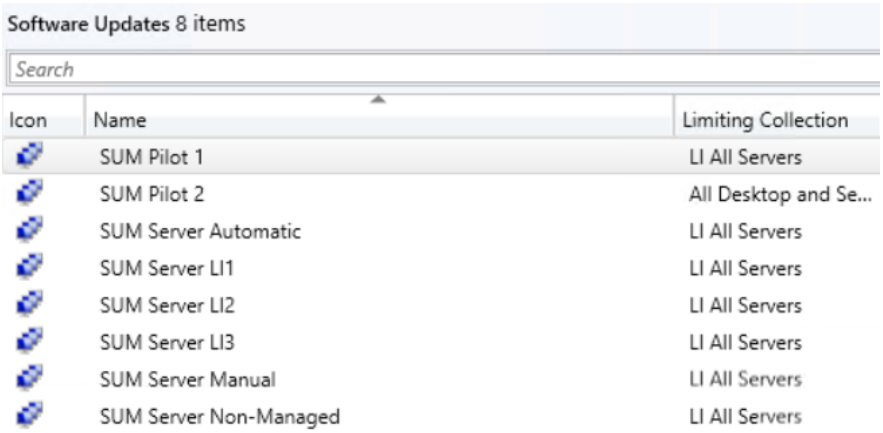
- **Pilot 1, Pilot 2** - Pilot 1 je využíván k prvotnímu otestování instalace aktualizací a restartování serverů. Pilot 2 je spouštěn po úspěšném dokončení Pilot 1. V této skupině jsou přiřazeny testovací stroje, u kterých by případný restart a neúspěšné aktualizace neznamenala vážnou ztrátu pro zbytek infrastruktury.

- **Automatic** - Skupina, ve které jsou přiřazeny servery, na kterých probíhají aktualizace v údržbových oknech. Skupina se skládá ze tří částí: LI1, LI2 a LI3. Do těchto skupin budou rozděleny všechny servery. Důvodem rozdělení do skupin je zamezení aktualizací primárních i sekundárních serverů, neboť by mohlo dojít k neúspěšné aktualizaci a to může mít za následek kolaps celé infrastruktury.

- **Manual** - Tato skupina je určena pro servery, na kterých se budou provádět aktualizace manuálně.

- **Non-managed** - Skupina určena pro servery, které nejsou v danou chvíli nijak spravovány.

Kolekce byly vytvořeny v Active Directory pomocí základního skriptu v Powershellu, který je uveden v knize [36]. Po přidání do Active Directory, musely být vytvořeny téže skupiny i v konfiguračním manažeru viz obrázek 7.5.



Obrázek 7.5: Software Update kolekce v konfiguračnímm manažeru

Pro kolekce Server LI1, LI2 a LI3 byly nastaveny jejich časy pro údržbu. V těchto oknech se mohou bezpečně instalovat softwarové aktualizace a restartovat, aniž by došlo k omezení provozu.

- **LI1** - každou neděli od 01:00 do 04:00

- **LI2** - každé pondělí od 01:00 do 04:00

- **LI3** - každou sobotu od 10:00 do 01:00

Je výhodné rozdělit tyto okna v závislosti na skupiny v Active Directory. *Maintenance Windows* se nastavuje pro každou skupinu zvlášť. Nastavení se provádí v konfiguračním manažeru v záložce*Assets and Compliance/Device Collection/Software Update*. Příklad je uveden na kolekci SUM Server LI1. Byly otevřeny vlastnosti pro tuto skupinu a v záložce Maintenance Window se po stisknutí žluté ikony otevřelo interaktivní okno, které slouží k nastavení názvu, času a jak často se má *Maintenance Windows* opakovat. Posledním nastavením *Maintenance Windows* bylo určení hlavní funkce tohoto okna. Zde byly zvoleny softwarové aktualizace. Tento krok byl proveden také u ostatních LI kolekcí.

7.3.2 Nastavení Software Update Pointu

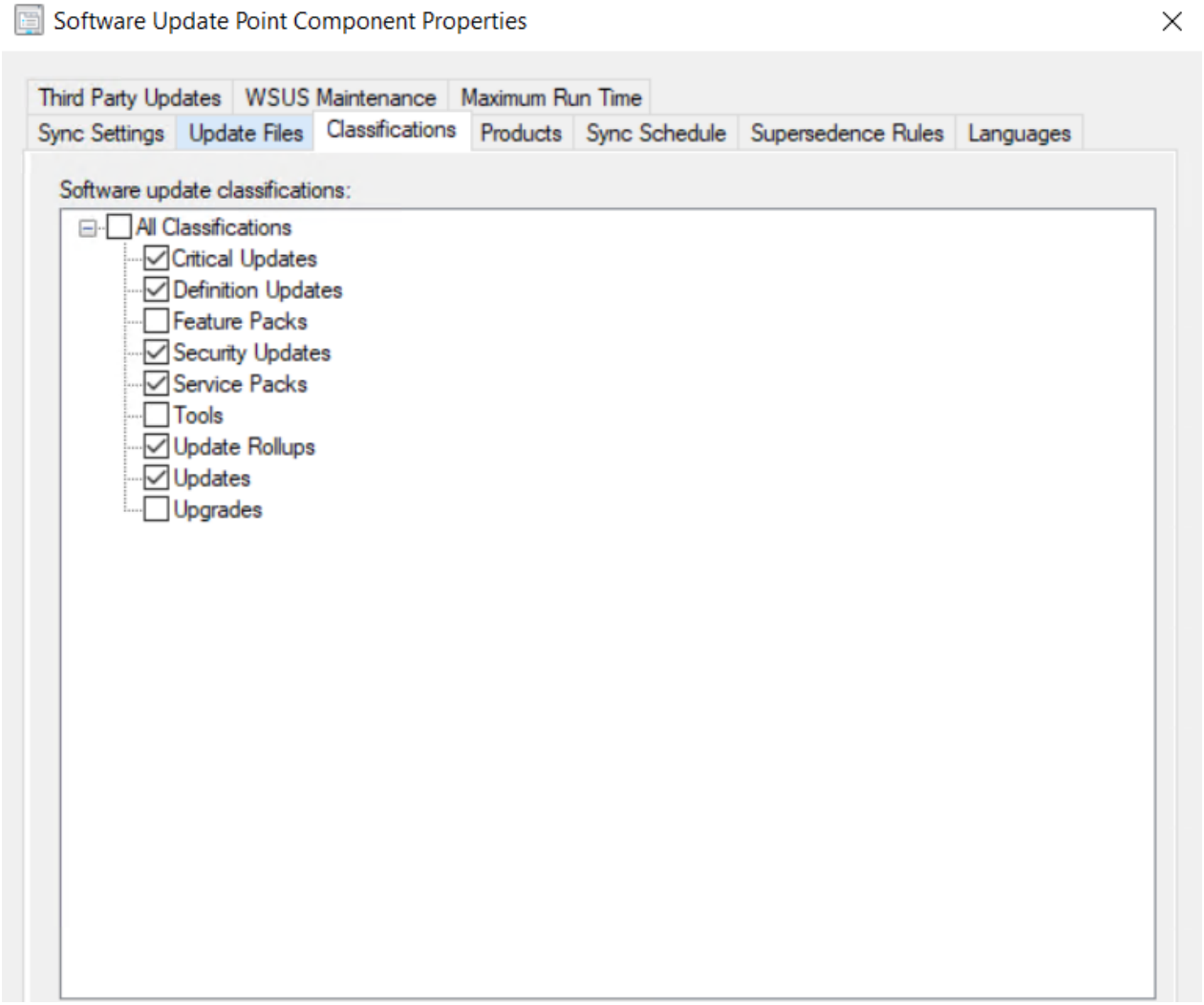
Po úspěšném rozvržení a vytvoření kolekcí, se přešlo k samotnému nastavení Software Update Pointu. Zde se muselo nastavit hned několik kroků. Nastavení je prováděno v *Administration/Sites*. Byl zvolen primární server, na kterém běží také WSUS a v záložce *Configure Site Component* byl zvolen právě Software Update Point. V záložce Sync Settings, byla povolena synchronizace s Microsoft Update serverem. V záložce *Classifications* byly vybrány typy balíčků, které se mají z Microsoft Update serveru stahovat viz obrázek 7.6.

- **Critical updates** obsahují vydanou opravu konkrétního problému, který řeší kritickou chybu, která však nesouvisí se zabezpečením.
- **Definition Updates** definují klasické aktualizace softwaru.
- **Security Updates** slouží pro opravu chyb v oblasti zabezpečení.
- **Update Rollups** je jednou z nejdůležitějších položek na tomto seznamu. Obsahuje testovanou kumulativní sadu oprav, aktualizaci zabezpečení, důležitých aktualizací a aktualizací, které jsou zabaleny do balíčků pro snadné nasazení.

Posledním krokem bylo vybrání produktů, které mají být stahovány službou WSUS. Toto bylo definováno v záložce *Products*, kde byly vybrány produkty, se kterými pracuje tato infrastruktura. Patří mezi ně: Windows Servery, Windows pro desktopy, Visual Studia, aktualizace pro SQL databázi a mnoho dalších. Od tohoto nastavení se pak odvíjí, jaké aktualizace budou využity při vytváření Automatic Deployment Rule.

7.3.3 Vytvoření Software Update Group

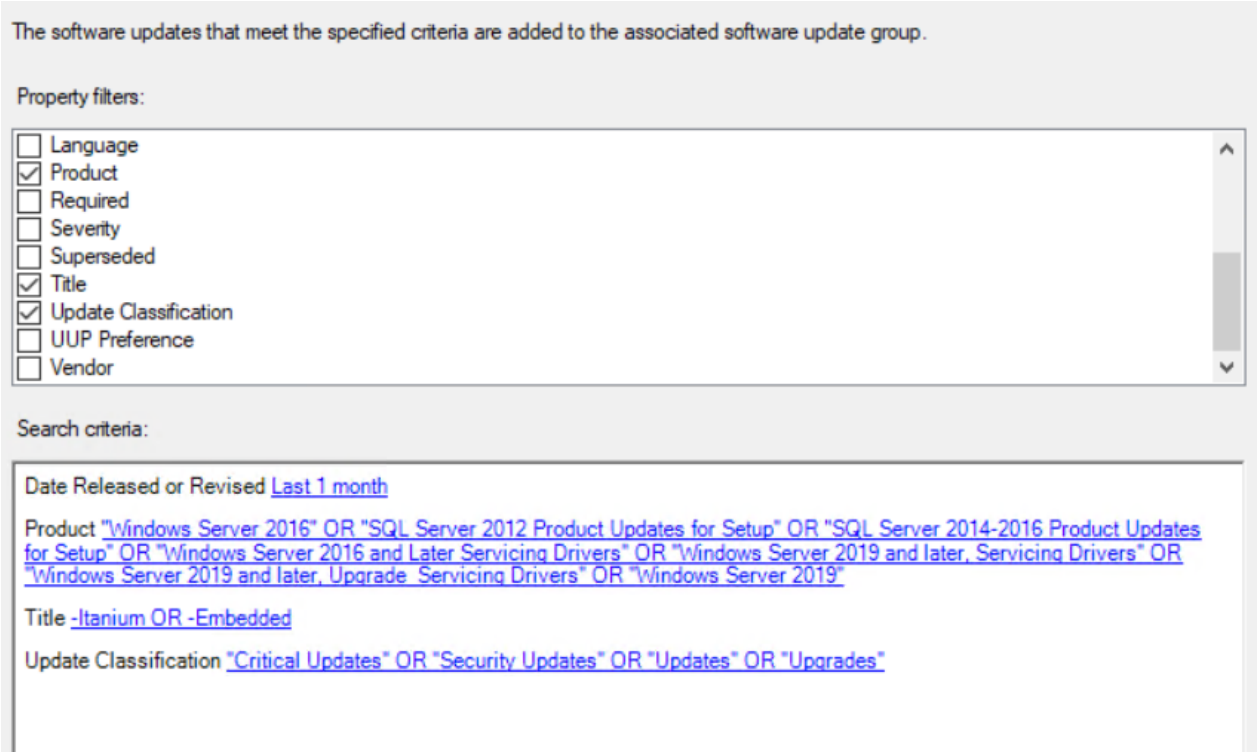
Automatické vytváření Software Update Groups velmi usnadňuje nasazení nových aktualizací na všechny stroje spravované v konfiguračním manažeru. Plně automatizovat aktualizace, není úplně správná volba, jelikož se při nahazování nových aktualizací mohou vyskytnout chyby, které mohou ovlivnit chod celé infrastruktury. Z tohoto důvodu jsou prováděny sekvenčně podle důležitosti běhu daného serveru v závislosti na infrastrukturu.



Obrázek 7.6: Základní architektura IDS

Automatic Deployment Rule se nachází v záložce *Software Library/Software updates/Automatic Deployment rule*. V konfiguračním wizardu bylo nutné nastavit několik kroků, které teď budou uvedeny. Na začátku je nutné specifikovat kolekci, které se bude aktualizační balíček týkat. Zde byla zvolena kolekce SUM Pilot 2. Tento krok není nijak zásadní, protože pro vytvořený balíček není zatím vytvořeno žádné nasazení. V kroku Software Updates byly zvoleny 4 kategorie Title, Date, Update Classification a Product. Na obrázku číslo 7.7 můžete vidět všechna kritéria, podle kterých jsou vybírány aktualizace do tohoto balíčku.

Pravidlo je spouštěno jednou měsíčně a to přesně druhou středu v měsíci, neboť každé druhé úterý v měsíci vydává Microsoft všechny důležité měsíční aktualizace. V konfiguračním wizardu nebylo řešeno žádné nastavení pro nasazení. Této části bude věnována pozornost až po dokončení konfigurace. V záložce *User Experience* byly pro uživatele schována všechna upozornění na chystané



Obrázek 7.7: Základní architektura IDS

aktualizace, aby žádný z uživatelů nemohl vynutit aktualizace stroje, mimo okénka údržby. Po dokončení bylo nutné pro toto pravidlo vytvořit nasazení pro každou přednastavenou kolekci.

Tento krok se taky provádí pomocí konfiguračního wizarda, který lze otevřít pravým kliknutím na dané pravidlo a zvolením Add deployment. Zde byla vybrána kolekce, na kterou se má nasadit tato skupina aktualizací. Důležité je, aby nasazení bylo ve výchozím stavu vypnuto. Tento krok byl dělán hlavně z důvodu usnadnění. Pokaždé, co se toto pravidlo spustí, automaticky se vytvoří nasazení na všechny kolekce a nemusí být ručně dodělávány každý měsíc.

7.3.4 Výsledek

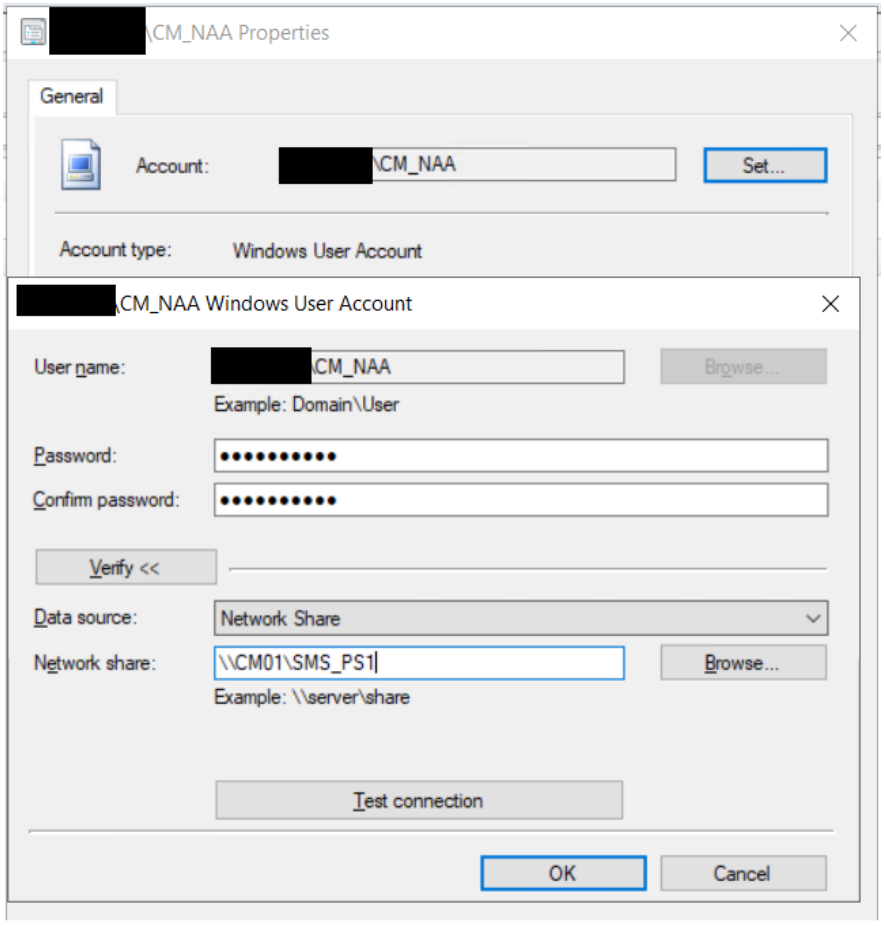
V předchozích kapitolách bylo popsáno, jak efektivně aktualizovat větší počet strojů pomocí konfiguračního manažera. Bylo dosaženo očekávaného výsledku a vytváření aktualizačních balíčku je plně funkční. Bylo nutné řešit řadu problémů, které se vyskytly během konfigurace. V prvotních krocích, vytvořené balíčky neobsahovaly žádné kumulativní aktualizace, což byl zásadní problém, který byl nutný vyřešit. To se nakonec podařilo po důkladném prohlédnutím nastavení produktů vybraných v Automatic Deployment Rule. Další kapitola se zaměří na konfiguraci nasazení automatické instalace Windows serveru s předem připraveným nastavením.

7.4 Automatické nasazení operačního systému

Nasazení operačního systému je jednou z nejpoužívanějších funkcí v konfiguračním manažeru. Aby se mohlo využívat nasazení operačních systémů, je nutné nastavit několik služeb. Prvním krokem je konfigurace požadované infrastruktury.

7.4.1 Konfigurace požadované infrastruktury

Předtím, než se začnou využívat funkce pro nasazování operačního systému, bylo nutné ověřit, že Network Access Account je v provozu. Network Access Account, dále jen NAA, je používán ke stanovení připojení z WinPE k distribučnímu bodu a stažení obrazu. Nastavení se provádí v konfiguračním manažeru v *Administration/Security/Accounts*. Zde se nachází účet CM_NAA. Ve vlastnostech účtu byl proveden test připojení síťového sdílení pro `//CM01/SMS_PS1`, jak je vidět na obrázku 7.8.



Obrázek 7.8: Otestování připojení CM_NAA

Dalším krokem byla instalace a konfigurace Windows Deployment Services, dále jen WDS. WDS je jen jedna z metod, jak můžou být nasazovány bitové kopie operačních systémů. WDS se nainstaluje automaticky po povolení funkce PXE na distribučním serveru. Tato část se nachází v konfiguračním manažeru v záložce *Administration/Distribution Points* ve vlastnostech primárního Site serveru. V záložce PXE, byla povolena PXE podporu pro klienty. Další parametry, které byly nutné pozměnit jsou:

- Povolení distribučnímu bodu odpovědi na příchozí PXE dotazy.
- Zapnutí podpory pro neznámé počítače.
- Nastavení hesla pro PXE bootování, neboť při povolení neznámých počítačů, by mohlo kdokoliv v interní síti vyslat požadavek o PXE boot a tím vzniká velké bezpečnostní riziko.

Aby mohlo být využito PXE bootování, musel být upraven také DHCP server. DHCP se v této infrastruktuře spravuje pomocí softwaru pfSense. Pro PXE boot z konfiguračního manažeru slouží specifická VLAN, ve které se nachází například server Build and Capture. V DHCP jsou dva důležité body, které musí být nastaveny. Prvním je povolení síťového bootování a druhým bodem je přiřazení Next Serveru. Jako next server, byla přiřazena IP adresa SCCM serveru. Po přiřazení adresy je nutná deklarace cesty, kde se má PXE odkázat. Byla uvedena tato cesta `SMSBoot//x64//wdsnbp.com`, která je typická pro bootování z konfiguračního manažeru. Tímto je PXE boot připraven a můžou být vytvářeny bootovací obrazy a Task sekvence.

Konfigurační manažer nabízí rozšířenou funkci, která obsahuje rozšířené funkce pro nasazení operačních systémů. Jedná se o službu Microsoft Deployment Toolkit zkráceně MDT. Tato funkce není součástí základní instalace a je jí nutné přidat manuálně. Tento balíček se dá stáhnout z oficiálních stránek Microsoftu. Poté se provede klasická instalace .msi balíčku. MDT nabízí dodatečné záznamy z procesu nasazení. Aby mohly být ukládány, je nutné vytvořit složku na disku a nastavit jí sdílení s primárním serverem. Poté se provede integrace s konfiguračním manažerem. Ten nám umožní vytváření MDT task sekvencí přímo v konfiguračním manažeru. Tato Task sekvence je složitější na konfiguraci, ale nabízí více možností oproti základní Task sekvenci. [36]

7.4.2 Boot Images

Bootovací obrazy jsou nezbytné pro nasazení operačních systémů. Bootovací obraz slouží ke stanovení spojení mezi počítačem a sítí. Obraz obsahuje verzi Windows PE, celým názvem *Windows Preinstallations Enviroment*, dále řadič síťového rozhraní a uložené ovladače a potřebnou logiku pro spuštění nasazovacího procesu, jako jsou skripty a další nástroje.

Konfigurační manažer má již v základu vytvořené dva bootovací obrazy pro architekturu x64 a x86. Oba tyto obrazy byly upraveny následujícím způsobem. Ve vlastnostech je záložka *Optional Components*, která umožní přidat možné komponenty, které budou tyto obrazy obsahovat. Zvoleny byly pouze dva komponenty a to Windows PowerShell a Microsoft .NET. V záložce *Customization*

byla změněna velikost odkládacího prostoru na 512MB a povolena podpora příkazů pro testovací účely. V záložce *Data Source* bylo nutné povolit možnost, aby tento bootovací obraz mohl být distribuován pomocí PXE.

Byly připraveny také bootovací obrazy, které se používají u MDT Task sekvencí. Ve File Exploreru byly vytvořeny dvě složky a jejich absolutní cesta je *Sources/OSD/Bootimages/MDTboot/*. V konfiguračním manažeru v záložce *Software Library/Operating Systems/Boot Images* byla zvolena možnost vytvoření nového bootovacího obrazu, který využívá MDT. V konfiguračním wizardu byla uvedena UNC cestu k vytvořeným složkám, jméno a verze bootovacího obrazu. V záložce *Options* byla uvedena platformu x64 a odkládací prostor byl změněn na 512MB. Dále bylo ponecháno defaultní nastavení a tento krok byl zopakován i pro platformu x86.

Po vytvoření bylo nutné provést úpravu, jako u základních bootovacích obrazů. Oba obrazy byly vybrány a byla provedena distribuce obsahu. V konfiguračním wizardu byl na záložce *Content Destination* zvolen Add/Distribution Poind Group a byl vybrán All Content. Tímto jsou připravené bootovací obrazy pro vytváření klasických Task sekvencí nebo MDT Task sekvencí.

7.4.3 Vytvoření vlastního WIM obrazu

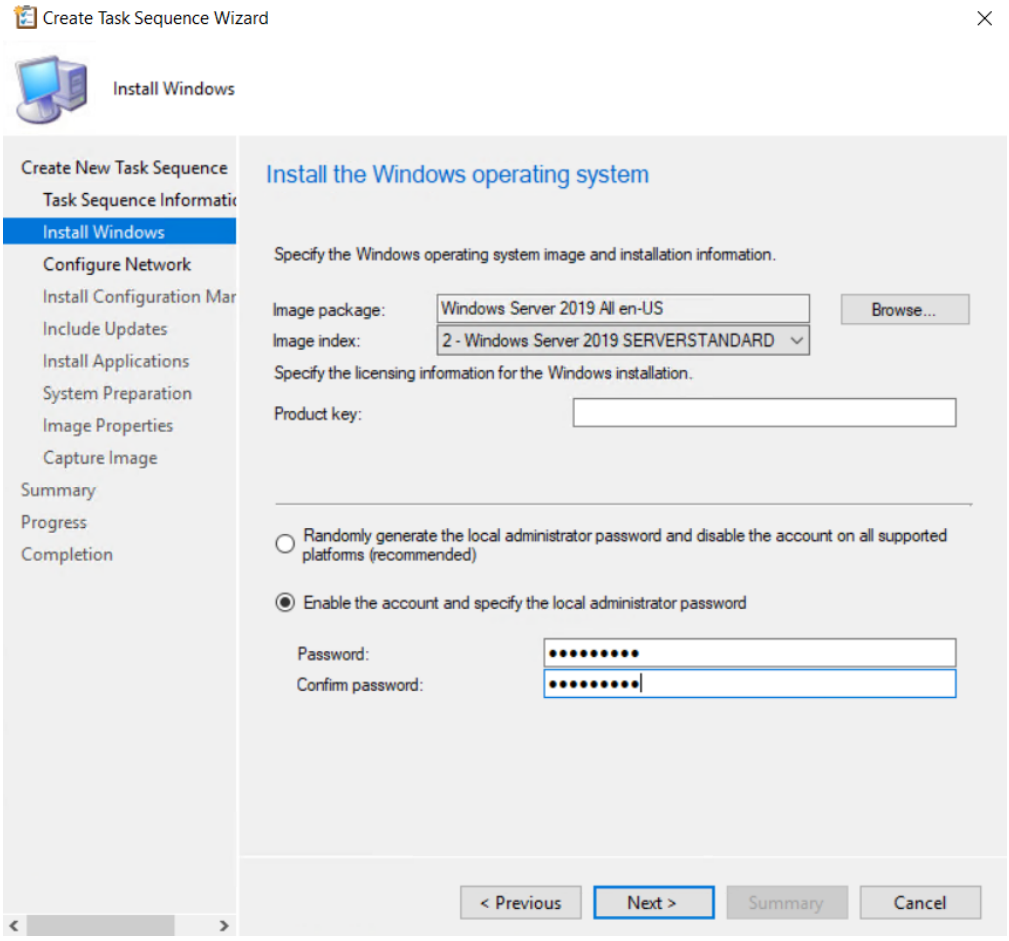
Pomocí konfiguračního manažera mohou být vytvořeny tři různé typy obrazů a to *thin, thick, hybrid*. Každá z těchto variant má nějaké výhody a nevýhody, které zde budou uvedeny.

- **Thin** - Obrazy typu *thin* neobsahují žádné aplikace. Aplikace se instalují separátně až po dokončení instalace obrazu. Výhodou tohoto typu je velká rychlost instalace, neboť je velmi malý. Obsahuje pouze operační systém a softwarové aktualizace.
- **Thick** - Obraz typu *thick* může obsahovat často používané aplikace. Výhodou tohoto typu je možnost okamžité práce s WIM obrazem po jeho dokončení bez nutnosti doinstalování dalších balíčků. Nevýhodou je správa těchto obrazů. Jedná se o komplexnější záležitost než u obrazů typu *thin*. Pokud totiž dojde k aktualizaci aplikací, je nutné obraz znovu vytvořit, aby se aktualizace projevili již ve vytvořeném WIM souboru. Další nevýhodou je i délka instalace samotného WIM obrazu.
- **Hybrid** - Obraz typu hybrid, jak je již z názvu zřejmé, kombinuje předchozí dva typy. Tento typ nám dovoluje aktualizovat aplikace bez nutnosti reinstalace WIM obrazu. [36]

Ještě než se začala vytvářet samotná Task sekvence, bylo nutné uvést zdroj pro operační systém. Na disku E: byla vytvořena složka OSInstall na absolutní adrese `Sources/OSD/OSInstall`, do které byly přidány bootovací obraz pro Windows Server 2019. Tímto krokem byly obrazy přidány na server, ale konfigurační manažer o něm zatím netušil. Proto bylo nutné přidat odkaz na tuto složku. V konfiguračním manažeru v *Software Library/Operating System Images* byly vytvořeny dvě složky Build and Capture a Deploy Production. Ve složce Build and Capture byl přidán obraz operačního systému. V konfiguračním wizardu v záložce Data Sources, byla uvedena sdílená cesta ke složce.

Poté byl obsah distribuován na všechny distribuční body. Nyní bylo vše připravené pro vytváření Task sekvencí.

V prvním kroku byla vytvořena složka, kde se budou ukládat vytvořené WIM obrazy. Opět byla vytvořena na disku E: ve složce `Sources/OSD/Images`. Této složce byly nutné přiřadit NTFS práva pro uživatel CM_NAA. Task sekvence se vytvářejí v konfiguračním manažeru v záložce *Software Library/Operation system/Task sequences*. Byly zde vytvořeny dvě složky pro oddělení testovacích sekvencí a sekvencí, které slouží pro nasazení. Ve složce Build and Capture byla vytvořena Task sekvence pomocí konfiguračního wizardu. Byla zvolena možnost pro vytvoření Build and Capture Reference operating system image. V další části bylo uvedeno jméno sekvence a byl zvolen bootovací obraz, který již byl vytvořen. V sekci Install Windows byly nutné upravit dvě věci. První bylo přiřadit připravený obraz Windows Serveru 2019. Produktový klíč se nechal nevyplněn a bylo nastaveno administrátorské heslo. Průběh instalace můžete vidět na obrázku 7.9.



Obrázek 7.9: Vytváření Task sekvence

V dalším bodě bylo zvoleno, ať se server připojí do interní domény pod administrátorským účtem. Je nutné, aby byl v doméně, neboť bez připojení do domény by neměl možnost instalovat

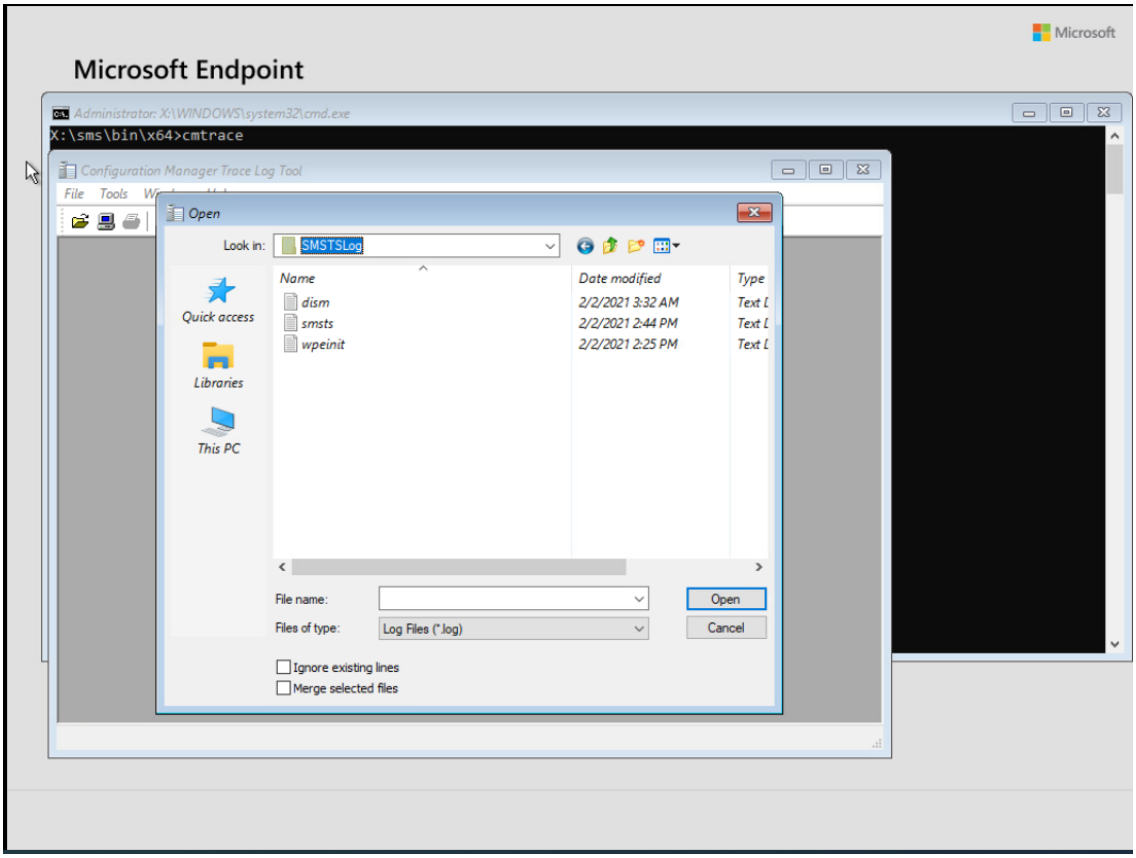
aplikace, které mu mohou být později přiřazeny. V následujících krocích byla zvolena instalace konfiguračního manažera s odkazem na primární server. Zvolena také byla instalaci všech softwarových aktualizací. Po tomto kroku následuje přidání aplikací, které se mají při instalaci WIM nainstalovat. Pro ukázku byla přidána aplikace 7-zip, kterou nejprve bylo nutné přidat do Software Library a vytvořit model pro nasazení aplikace. Poslední záložkou je Capture Image, kde byl přidán odkaz na předem vytvořenou složku. Jako obvykle cesta ke složce je sdílená na //cm01/.

Po dokončení konfigurace Task sekvence je nutné vyřešit její nasazení. Nastavení nasazení obsahuje pár důležitých bodů, jedním z těchto bodů je výběr cílové kolekce. Pro tuto funkci se skvěle hodí kolekce All Unknown Computers, jelikož stroje, které tuto funkci využívají obvykle nejsou součástí domény. Další parametry definují, co se má s danou Task sekvencí provádět. Proto byla zvolena, aby došlo k provedení instalace, když bude dostupná a pouze za využití PXE bootování.

Tímto je vše připravené pro vytvoření WIM obrazu. Ve webovém prohlížeči byl pomocí softwaru VMware vytvořen virtuální server Build and Capture. Tomuto serveru byly přiřazeny 4 procesory, 6GB operační paměti a 40GB místa na disku. Byla mu přiřazena síťová karta, které slouží pro VLAN, která má konfiguraci pro PXE bootování z konfiguračního manažeru. Po zapnutí stroje bylo vyvoláno bootování pomocí PXE a byla získána odezva od primárního serveru CM01 a pomocí klávesy F12 byl stažen bootovací obraz. Došlo k spuštění Task Sequence Wizard, kde bylo na výběr z předem připravených Task sekvencí. Po zvolení začne probíhat celá instalace automaticky. Virtuální server se během instalace několikrát restartuje. Instalace je celkem zdlouhavá, její trvání je něco okolo hodiny. Doba se však odvíjí od počtu kroků v Task sekvenci.

Během této instalace se vyskytla řada chyb, které bylo nutné opravit a tento proces opakovat. Pro nalezení těchto chyb byly využity výpisu logů, které se dají otevřít přímo na virtuálním počítači viz obrázek 7.10.

Bootovací obraz v sobě obsahuje i nástroj CMTrace, který procházení daných logů značně usnadní. Pro spuštění těchto logů se používá příkazový řádek, který je možné spustit pomocí klávesy F8. Zde je použit příkaz `cmtrace.exe`, který spustí tuto aplikaci. Logy se nachází na disku C: ve složce *SMSTSLOG*. Ten nejužitečnější z nich se jmenuje `smsts.log`. V tomto logu jsou zaznamenávány všechny aktivity, které jsou vykonávány během instalace.



Obrázek 7.10: Ukázka dostupných logů při instalaci WIM

Kapitola 8

Závěr

V rámci této diplomové práce došlo k seznámení s nástroji, které vytváří bezpečnostní audity v síťové infrastruktuře. Byly představeny silné a slabé stránky používaných IDS nástrojů a byly také představeny nástroje zabývající se skenováním zranitelnosti na serverech. Větší část práce je věnovaná automatizované správě Windows serverů. Byly uvedeny nástroje používané pro automatizovanou správu ve větších infrastrukturách a detailněji byl popsán nástroj System Center Configuration Manager.

Byla provedena instalace a konfigurace nástroje OpenVAS. Byla popsána detailní konfigurace pro pravidelné skenování vzniklých bezpečnostních zranitelností. Jsou zde uvedeny metody, které lze pro skenování zranitelností v systémů používat a byly představeny metody pro okamžité upozornění na vzniklou chybu. V diplomové práci je také popsán rozbor výsledků testování.

V další části práce byla popsána instalace a konfigurace nástroje Suricata, která zastává funkce IDS nástroje. Byly představeny nabízené globální funkce a využití různých sad pravidel. Byla uvedena podrobná konfigurace pro možnost nasazení IDS nástroje na síťová rozhraní. V diplomové práci jsou popsána použitá pravidla, které pokrývají nejpodstatnější část síťového provozu. V závěru kapitoly byly představeny výsledné výpisy záznamů zachycené při běžném síťovém provozu.

Druhou částí diplomové práce byla implementace automatizované správy systémů se zaměřením na systémy od společnosti Microsoft. Byl využit software System Center Configration Manager, který je pro správu systému od společnosti Microsoft ideální. V úvodu této kapitoly byl popsán proces instalace softwaru. Instalace zahrnovala přípravu prostředí před samotnou instalací, instalaci SQL serveru, který je součástí primárního Site serveru a samotnou instalaci konfiguračního manažera. System Center Configuration Manager musel být po nainstalování pečlivě nakonfigurován, aby mohly být správně využívány jeho funkce. Bylo nutné provést instalaci systémových rolí a konfigurace úkolů údržby. Byl nastaven proces Discovery pro vyhledávání zdrojů, který má za úkol hledat základní informace o objektech. Poslední částí počáteční konfigurace bylo správné rozdělení kolekcí, které jsou hlavním orientačním bodem v automatické správě systémů v tomto softwaru.

První nastavovanou funkcí bylo automatické nasazení aktualizací pro operační systémy Windows. Byly představeny použité kolekce, které jsou používány pro nasazení těchto aktualizací. Nastavením Software Update Pointu se definovaly, jaké aktualizace mají být stahovány. Následujícím krokem bylo utvoření skupiny Software Update, která jednou měsíčně stáhne vybrané aktualizace a postupně je nainstaluje na všechny servery v určených dobách údržby. Bylo tak docíleno automatické aktualizace všech serverů, čím se zajistila větší bezpečnost těchto strojů. Poslední funkcí bylo automatické nasazení operačních systémů, které byly po instalaci připojeny do domény. Došlo k úpravě nastavení pro rozhraní v DHCP serveru, aby bylo povoleno bootování pomocí PXE. Cílem bylo vytvořit vlastní WIM obraz, který bude po doinstalování připojen do domény s předpřipraveným nastavím. Tohoto cíle bylo úspěšnou konfigurací docíleno.

Nástroj System Center Configuration Manager je velice komplexní nástroj, který by si zasloužil mnohem hlubší studium, aby byly využity téměř všechny funkce, které nástroj nabízí. Jeho nasazení je velmi podstatné, pokud běží na dané infrastruktuře velký počet serverů s operačním systémem Windows. Počet nezbytných úkonů pro správu narůstá a nelze je zvládnout v přijatelném časovém rozsahu bez využívání softwaru pro správu systémů.

Literatura

1. EASTTOM, Chuck. *Network Defense and Countermeasures: Principles and Practices, Third edition*. Pearson IT Certification, [n.d.]. Dostupné také z: https://www.oreilly.com/library/view/network-defense-and/9780134893112/.
2. RADWARE. *History of Network Security Methods*. [N.d.]. Dostupné také z: https://www.radware.com/resources/network_security_history.aspx.
3. COX, Kerry; GERG, Christopher. *Managing security with Snort and IDS tools*. OReilly Media, 2004.
4. *Whats IT automation?* [N.d.]. Dostupné také z: https://www.redhat.com/en/topics/automation/whats-it-automation.
5. COMMENTARY, Guest. *5 Must-Have IT Infrastructure Automation Tools*. Information Week, 2019-11. Dostupné také z: https://www.informationweek.com/big-data/5-must-have-it-infrastructure-automation-tools/a/d-id/1336345.
6. LASTER, BRENT. *JENKINS X: creating automated cloud-ready ci/cd pipelines*. OREILLY MEDIA, 2020.
7. ACZECHOWSKI. *Co je Configuration Manager? - Configuration Manager*. [N.d.]. Dostupné také z: https://docs.microsoft.com/cs-cz/mem/configmgr/core/understand/introduction.
8. SCIONTI, Alberto; MARTINOVIC, Jan; TERZO, Olivier; WALTER, Etienne; LEVRIER, Marc; HACHINGER, Stephan; MAGARIELLI, Donato; GOUBIER, Thierry; LOUISE, Stephane; PARODI, Antonio; AL., et. HPC, Cloud and Big-Data Convergent Architectures: The LEXIS Approach. *Advances in Intelligent Systems and Computing Complex, Intelligent, and Software Intensive Systems*. 2019, s. 200–212. Dostupné z DOI: 10.1007/978-3-030-22354-0_19.
9. GAVANDA, MARTIN. *MASTERING VMWARE VSPHERE 6.7 -: effectively virtualize, administer, manage, and monitor ... your data centers with vmware vsphere 6.7*. PACKT Publishing Limited, 2019.

10. KHEDHER, Omar. *Mastering OpenStack: discover your complete guide to designing, deploying, and managing OpenStack-based clouds in mid-to-large IT infrastructures with best practices, expert understanding, and more*. Packt Publishing, 2017.

11. *Open Source Cloud Computing Platform Software*. [N.d.]. Dostupné také z: `https://www.openstack.org/software/`.

12. *A quick overview of OpenStack technology*. 2019-02. Dostupné také z: `https://www.ibm.com/blogs/cloud-computing/2014/08/06/quick-overview-openstack-technology/`.

13. ZIENTARA, DAVID. *LEARN PFSENSE 2.4: get up and running with pfsense and all the core concepts to build firewall and. routing solutions*. PACKT Publishing Limited, 2018.

14. FRANCIS, Dishan. *Mastering Active Directory*. Packt Publishing, [n.d.]. Dostupné také z: `https://www.oreilly.com/library/view/mastering-active-directory/9781787289352/`.

15. *Kismet Wireless*. [N.d.]. Dostupné také z: `https://www.kismetwireless.net/`.

16. *SANS Institute: Reading Room - Intrusion Detection*. [N.d.]. Dostupné také z: `https://www.sans.org/reading-room/whitepapers/detection/inexpensive-wireless-ids-kismet-openwrt-33103`.

17. *1. What is Sagan?* [N.d.]. Dostupné také z: `https://sagan.readthedocs.io/en/latest/what-is-sagan.html`.

18. MESSIER, Ric. *Network forensics*. Wiley, 2017.

19. *What is Suricata IDS?* 2020-10. Dostupné také z: `https://bricata.com/blog/what-is-suricata-ids/`.

20. COX, Kerry; GERG, Christopher. *Managing security with Snort and IDS tools*. OReilly Media, 2004.

21. *Hyperscan and Snort* Integration*. [N.d.]. Dostupné také z: `https://software.intel.com/content/www/us/en/develop/articles/hyperscan-and-snort-integration.html`.

22. *SolarWinds Security Event Manager Review - Best SEIM Tool of 2020!* 2020-06. Dostupné také z: `https://www.networkmanagementsoftware.com/solarwinds-security-and-event-manager-review/`.

23. *FAQ: What is CrowdStrike?: Platform, Products and More*. 2021-01. Dostupné také z: `https://www.crowdstrike.com/endpoint-security-products/crowdstrike-falcon-faq/`.

24. *Open Vulnerability Assessment Scanner*. [N.d.]. Dostupné také z: `https://www.openvas.org/`.

25. *OpenVAS*. Wikimedia Foundation, 2021-03. Dostupné také z: `https://en.wikipedia.org/wiki/OpenVAS`.

26. RAHALKAR, Sagar. *Quick Start Guide to Penetration Testing With NMAP, OpenVAS and Metasploit*. Apress, 2019.

27. *OpenVAS Vulnerability Scanner Online*. 2020-04. Dostupné také z: https://hackertarget.com/openvas-scan/.

28. CYBERSECURITYLABS; CYBERSECURITYLABS. *Introduction to Nessus Vulnerability Scanner*. 2014-03. Dostupné také z: https://cybersecuritylabs.wordpress.com/2014/02/03/nessus-vulnerability-scanner/.

29. ROGERS, Russ. *Nessus Network Auditing, 2nd Edition*. Syngress, [n.d.]. Dostupné také z: https://www.oreilly.com/library/view/nessus-network-auditing/9781597492089/.

30. *About Nessus*. [N.d.]. Dostupné také z: https://docs.tenable.com/nessus/Content/SettingsAbout.htm.

31. RUECKER, BERND. *PRACTICAL PROCESS AUTOMATION: orchestration and integration in microservices and cloud native... architectures*. O'REILLY MEDIA, 2021.

32. MCKENDRICK, RUSS. *LEARN ANSIBLE: automate cloud, security, and network infrastructure using ansible 2.x*. PACKT Publishing Limited, 2018.

33. ANSIBLE, Red Hat. *How Ansible Works*. [N.d.]. Dostupné také z: https://www.ansible.com/overview/how-ansible-works.

34. *Citrix Systems*. Wikimedia Foundation, 2021-02. Dostupné také z: https://en.wikipedia.org/wiki/Citrix_Systems.

35. [N.d.]. Dostupné také z: https://docs.citrix.com/en-us/citrix-workspace.html.

36. AGERLUND, Kent. *System Center 2012 R2 Configuration Manager: Mastering the Fundamentals, 3rd Edition*. Deployment Artist, 2014.

37. *SCCM (System Center Configuration Manager)*. 2019-09. Dostupné také z: https://tudip.com/blog-post/sccm-system-center-configuration-manager/.

38. KELLEY, Shaun. *What is SCCM and How Does it Work?* Automox, 2021-01. Dostupné také z: https://blog.automox.com/what-is-sccm.

39. *10. Scanning a System¶*. [N.d.]. Dostupné také z: https://docs.greenbone.net/GSM-Manual/gos-6/en/scanning.html?highlight=type%20scanner.

40. *ET Category Descriptions*. [N.d.]. Dostupné také z: https://tools.emergingthreats.net/docs/ETPro%5C%20Rule%5C%20Categories.pdf.